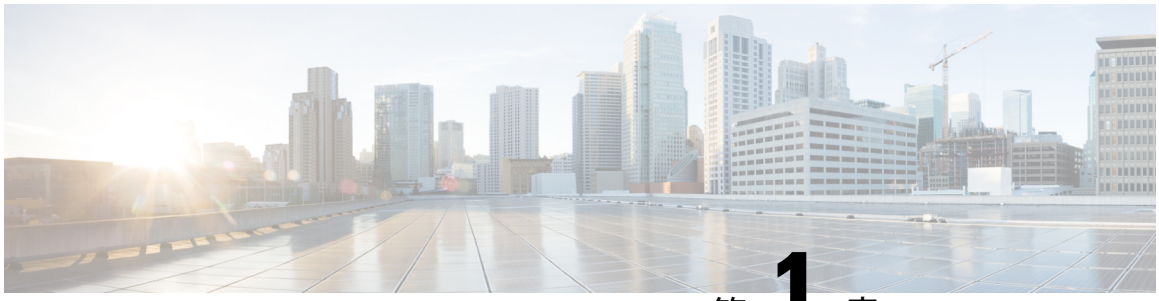
Cisco ASA アップグレードガイド

最終更新：2020 年 4 月 21 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

© 2021 Cisco Systems, Inc. All rights reserved.

目 次



第 1 章

アップグレードの計画

ASA をアップグレードする前に、次の準備を行う必要があります。

- 異なるバージョンのオペレーティング システム間の互換性を確認します。たとえば、ASA のバージョンと ASA FirePower モジュールのバージョンに互換性があることを確認します。
- 現在のバージョンのターゲット バージョンへのアップグレード パスを確認します。必ず、各オペレーティン グシステムに必要な中間バージョンについて計画してください。
- 中間バージョンとターゲット バージョンに関係するガイドラインおよび制限事項、またはフェールオーバーとクラスタリングのゼロ ダウンタイム アップグレードに関係するガイドラインおよび制限事項を確認します。
- Cisco.com から必要なすべてのソフトウェア パッケージをダウンロードします。
- 設定をバックアップします（特に設定を移行する場合）。

ここでは、ASA をアップグレードする方法について説明します。

ASA アップグレードのチェックリスト

アップグレードを計画する際は、次のチェックリストを使用してください。

1. ASA のモデル（ASA のアップグレードパス （33 ページ））：_____

   現在の ASA のバージョン（ASA のアップグレードパス （33 ページ））：_____

2. モデルごとの ASA/ASDM の互換性をチェックします（モデルごとの ASA と ASDM の互換性 （4 ページ））。

   ターゲット ASA のバージョン：_____

   ターゲット ASDM のバージョン：_____

3. ASA（ASA のアップグレードパス （33 ページ））のアップグレード パスをチェックします。必要な中間バージョンはありますか。はい _____ いいえ _____

   「はい」の場合、ASA の中間バージョン：

   _____

4. ターゲット バージョンおよび中間バージョンの ASA/ASDM をダウンロードします（ASA ソフトウェアのダウンロード （51 ページ））。

（注） ASDM は ASA for FXOS パッケージに含まれています。

5. ASA FirePOWER モジュールはありますか。はい _____ いいえ _____

   「はい」の場合：

   1. 現在の ASA FirePOWER のバージョン：_____

      現在のバージョンを表示します：ASDM（ASA FirePOWER ASDM によるアップグレード パス （42 ページ））または Firepower Management Center（アップグレードパス：Firepower Management Center （46 ページ））。

   2. ASA/FirePOWER の互換性をチェックします（ASA と ASA FirePOWER モジュールの互換性 （9 ページ））。

      ASA FirePOWER のターゲット バージョン：_____

   3. ASA FirePOWER のアップグレード パスをチェックします（ASA FirePOWER ASDM によるアップグレード パス （42 ページ）または Asa FirePOWER アップグレードパス：FMC 搭載アップグレードパス：ASA FirePOWER （44 ページ））。必要な中間バージョンはありますか。はい _____ いいえ _____

      「はい」の場合、ASA FirePOWER の中間バージョン：

      _____

   4. ターゲット バージョンおよび中間バージョンの ASA FirePOWER をダウンロードします（ASA FirePOWER ソフトウェアのダウンロード （60 ページ））。

   5. Firepower Management Center を使用してモジュールを管理しますか。はい _____ いいえ _____

      「はい」の場合：

      1. Firepower Management Center のモデル（アップグレードパス：Firepower Management Center （46 ページ））：_____

現在の Firepower Management Center のバージョン（アップグレードパス：Firepower Management Center （46 ページ））：_____

2. Firepower Management Center のアップグレード パスをチェックします（アップグレードパス：Firepower Management Center （46 ページ））。必要な中間バージョンはありますか。はい _____ いいえ _____

   「はい」の場合、ASA FirePOWER の中間バージョン：

   _____

3. Firepower Management Center と管理対象デバイスの互換性をチェックします（FMC デバイスのバージョン互換性を維持できるか （22 ページ））。必ず、Firepower Management Center のアップグレードに合わせた ASA FirePOWER モジュールのアップグレードを計画してください。

4. Firepower Management Center 用のターゲットバージョンおよび中間バージョンをダウンロードします（FMC Upgrade Guide）。

6. ASA のモデルは Firepower 4100 または 9300 ですか。はい _____ いいえ _____

   「はい」の場合：

   1. 現在の FXOS のバージョン（アップグレードパス：Firepower 4100/9300 シャーシ上の FXOS （48 ページ））：_____

   2. ASA/Firepower 4100 および 9300 の互換性をチェックします（Firepower 4100/9300 と ASA または FTD の互換性 （24 ページ））。

      FXOS のターゲット バージョン：_____

   3. FXOS のアップグレード パスをチェックします（アップグレードパス：Firepower 4100/9300 シャーシ上の FXOS （48 ページ））。必要な中間バージョンはありますか。はい _____ いいえ _____

      「はい」の場合、FXOS の中間バージョン：

      _____

      互換性を維持するために、必ず、FXOS のアップグレードに合わせた ASA のアップグレードを計画してください。

      アップグレード時に互換性を維持するために必要な ASA の中間バージョン：

      _____

   4. ターゲット バージョンおよび中間バージョンの FXOS をダウンロードします（アップグレード パッケージの Firepower 4100/9300 シャーシFXOS （64 ページ））。

      中間バージョンの ASA をダウンロードします（ASA ソフトウェアのダウンロード （51 ページ））。

   5. Radware DefensePro デコレータ アプリケーションを使用しますか。はい _____ いいえ _____

      「はい」の場合：

1. 現在の DefensePro のバージョン：_____
2. ASA/FXOS/DefensePro の互換性をチェックします（Radware DefensePro の互換性（31 ページ））。

   DefensePro のターゲット バージョン：_____
3. ターゲット バージョンの DefensePro をダウンロードします。

7. 各オペレーティング システムのアップグレード ガイドラインをチェックします。
   - ASA のアップグレード ガイドライン （65 ページ）。
   - ASA FirePOWER ガイドライン：『FMC Upgrade guide』を参照してください。
   - Firepower Management Center ガイドライン：『FMC Upgrade guide』を参照してください。
   - FXOS ガイドライン：各中間およびターゲット バージョンの『FXOS リリース ノート』を参照してください。
8. 設定をバックアップします。バックアップの方法については、各オペレーティング システムの設定ガイドを参照してください。

互換性

このセクションには、プラットフォーム、オペレーティング システム、およびアプリケーション間の互換性を示す表があります。

モデルごとの ASA と ASDM の互換性

次の表に、現在のモデルに関する ASA と ASDM の互換性を示します。古いバージョンおよびモデルについては、『Cisco ASA Compatibility』を参照してください。

ASA 9.14 から 9.13

太字のリリースは推奨バージョンです。

（注） ASA 9.14(x) は ASA 5525-X、5545-X、および 5555-X の最終バージョンです。

ASA 9.12(x) は ASA 5512-X、5515-X、5585-X、および ASASM 用の最終バージョン、

特に明記されていない限り、ASDM のバージョンは以前のすべての ASA のバージョンと下位互換性があります。たとえば、ASDM 7.13(1) は ASA 9.10(1) で ASA 5516-X を管理できます。ASDM 7.13(1) と 7.14(1) は、ASA 5512-X、5515-X、5585-X、および ASASM をサポートしていませんでした。そのため、ASDM 7.13(1.101) または 7.14(1.48) にアップグレードして ASDM のサポートを復元する必要があります。

表 *1 : ASA* と *ASDM* の互換性：*9.14* から *9.13*

ASA	ASDM	ASA モデル							
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5525-X 5545-X 5555-X	ASAv	Firepower 1010 1120 1140 1150	Firepower 2110 2120 2130 2140	Firepower 4110 4112 4115 4120 4125 4140 4145 4150	Firepower 9300	ISA 3000
9.14(1.30)	7.14(1.48)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.14(1.6)	7.14(1.48)	—	—	**YES** (+ASAv100)	—	—	—	—	—
9.14(1)	7.14(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.13(1)	7.13(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**（4112 を除く）	**YES**	**YES**

ASA 9.12 から 9.5

太字のリリースは推奨バージョンです。

（注） ASA 9.12(x) は ASA 5512-X、5515-X、5585-X、および ASASM 用の最終バージョン、

特に明記されていない限り、ASDM のバージョンは以前のすべての ASA のバージョンと下位互換性があります。たとえば、ASDM 7.12(1) は ASA 9.10(1) で ASA 5515-X を管理できます。

表 *2 : ASA* と *ASDM* の互換性：*9.12* から *9.5*

ASA	ASDM	ASA モデル									
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5512-X 5515-X 5525-X 5545-X 5555-X	ASA 5585-X	ASAv	ASASM	Firepower 2110 2120 2130 2140	Firepower 4110 4120 4140 4150	Firepower 4115 4125 4145	Firepower 9300	ISA 3000
9.12(4)	7.13(1.101)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.12(3)	7.12(2)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.12(2)	7.12(2)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.12(1)	7.12(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.10(1)	7.10(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	**YES**
9.9(2)	7.9(2)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	**YES**
9.9(1)	7.9(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	**YES**
9.8(4)	7.12(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	**YES**
9.8(3)	7.9(2.152)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	**YES**
9.8(2)	7.8(2)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	**YES**
9.8(1.200)	サポートなし	—	—	—	**YES**	—	—	—	—	—	—
9.8(1)	7.8(1)	**YES**	**YES**	**YES**	**YES**（ASA 5506-X を除く）	**YES**	—	**YES**	—	**YES**	**YES**
9.7(1.4)	7.7(1)	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	—	**YES**	**YES**
9.6(4)	7.9(1)	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	—	**YES**	**YES**
9.6(3.1)	7.7(1)	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	—	**YES**	**YES**
9.6(2)	7.6(2)	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	—	**YES**	**YES**
9.6(1)	7.6(1)	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**（4150 を除く）	—	**YES**	**YES**
9.5(3.9)	7.6(2)	**YES**	**YES**	**YES**	**YES**	**YES**	—	—	—	—	**YES**

ASA	ASDM	ASA モデル									
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5512-X 5515-X 5525-X 5545-X 5555-X	ASA 5585-X	ASAv	ASASM	Firepower 2110 2120 2130 2140	Firepower 4110 4120 4140 4150	Firepower 4115 4125 4145	Firepower 9300	ISA 3000
9.5(2.200)	7.5(2.153)	—	—	—	YES	—	—	—	—	—	—
9.5(2.2)	7.5(2)	—	—	—	—	—	—	—	—	YES	—
9.5(2.1)	7.5(2)	—	—	—	—	—	—	—	—	YES	—
9.5(2)	7.5(2)	YES	YES	YES	YES	YES	—	—	—	—	YES
9.5(1.200)	7.5(1)	—	—	—	YES	—	—	—	—	—	—
9.5(1.5)	7.5(1.112)	YES	YES	YES	YES	YES	—	—	—	—	—
9.5(1)	7.5(1)	YES	YES	YES	YES	YES	—	—	—	—	—

ASA 9.4 から 9.3

（注） ASA 9.2(x) は ASA 5505 用の最終バージョン、以降のバージョンの ASDM では、ASA 5505 が引き続きサポートされています。

特に明記されていない限り、ASDM のバージョンは以前のすべての ASA のバージョンと下位互換性があります。たとえば、ASDM 7.6(2) は ASA 9.3(3) で ASA 5516-X を管理できます。

表 *3 : ASA* と *ASDM* の互換性：*9.4* から *9.3*

ASA	ASDM	ASA モデル						
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5512-X 5515-X 5525-X 5545-X 5555-X	ASA 5585-X	ASAv	ASASM	Firepower 9300	ISA 3000
9.4(4.5)	7.6(2)	YES	YES	YES	YES	YES	—	—
9.4(3)	7.6(1)	YES	YES	YES	YES	YES	—	—

ASA	ASDM	ASA モデル						
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5512-X 5515-X 5525-X 5545-X 5555-X	ASA 5585-X	ASAv	ASASM	Firepower 9300	ISA 3000
9.4(2.146)	7.5(1.112)	—	—	—	—	—	YES	—
9.4(2.145)	7.5(1.112)	—	—	—	—	—	YES	—
9.4（2）	7.5(1)	YES	YES	YES	YES	YES	—	—
9.4(1.225)	7.5(1)	—	—	—	—	—	—	YES
9.4(1.200)	7.4(2)	—	—	—	YES	—	—	—
9.4(1.152)	7.4(3)	—	—	—	—	—	YES	—
9.4(1)	7.4(1)	YES	YES	YES	YES	YES	—	—
9.3(3.8)	7.4(1)	YES	YES	YES	YES	YES	—	—
9.3(3)	7.4(1)	YES	YES	YES	YES	YES	—	—
9.3(2.200)	7.3(2)	—	—	—	YES	—	—	—
9.3(2)	7.3 (3)	はい（5506-X のみ）	YES	YES	YES	YES	—	—
	7.3(2)	はい（5506-X のみ）	YES	YES	YES	YES	—	—
9.3(1)	7.3(1)	—	YES	YES	YES	YES	—	—

ASA 9.2 から 9.1

（注） ASA 9.2(x) は ASA 5505 用の最終バージョン、以降のバージョンの ASDM では、ASA 5505 が引き続きサポートされています。

特に明記されていない限り、ASDM のバージョンは以前のすべての ASA のバージョンと下位互換性があります。たとえば、ASDM 7.4(3) は ASA 9.1(1) で ASA 5505 を管理できます。

表 *4 : ASA* と *ASDM* の互換性：*9.2* から *9.1*

ASA	ASDM	ASA モデル				
		ASA 5505	ASA 5512-X 5515-X 5525-X 5545-X 5555-X	ASA 5585-X	ASAv	ASASM
9.2(4.5)	7.4(3)	**YES**	**YES**	**YES**	**YES**	**YES**
9.2(4)	7.4(3)	**YES**	**YES**	**YES**	**YES**	**YES**
9.2(3)	7.3(1.101)	**YES**	**YES**	**YES**	**YES**	**YES**
9.2(2.4)	7.2(2)	**YES**	**YES**	**YES**	**YES**	**YES**
9.2(1)	7.2(1)	**YES**	**YES**	**YES**	**YES**	**YES**
9.1(7.4)	7.5(2)	**YES**	**YES**	**YES**	—	**YES**
9.1(6)	7.1(7)	**YES**	**YES**	**YES**	—	**YES**
9.1(5)	7.1(6)	**YES**	**YES**	**YES**	—	**YES**
9.1(4)	7.1(5)	**YES**	**YES**	**YES**	—	**YES**
9.1(3)	7.1(4)	**YES**	**YES**	**YES**	—	**YES**
9.1(2)	7.1(3)	**YES**	**YES**	**YES**	—	**YES**
9.1(1)	7.1(1)	**YES**	**YES**	**YES**	—	**YES**

ASA と ASA FirePOWER モジュールの互換性

互換性一覧表

次の表に ASA、ASDM、および ASA FirePOWER のサポートを示します。

（注） ASA 9.14(x)/ASDM 7.14(x)/FirePOWER 6.6 は ASA 5525-X、5545-X、および 5555-X の最終バージョンです。

ASA 9.12(x)/ASDM 7.12(x)/FirePOWER 6.4 は ASA 5515-X および 5585-X の最終バージョンです。

特に明記されていない限り、ASDM のバージョンは以前のすべての ASA のバージョンと下位互換性があります。たとえば、ASDM 7.13(1) は ASA 9.10(1) で ASA 5516-X を管理できます。ASDM 7.13(1) と 7.14(1) は、ASA 5512-X、5515-X、5585-X、および ASASM をサポートしていませんでした。そのため、ASDM 7.13(1.101) または 7.14(1.48) にアップグレードして ASDM のサポートを復元する必要があります。

表 *5: ASA* と *ASA FirePOWER* の互換性

ASA FirePOWER のバージョン	**ASDM** のバージョン（ローカル管理用）	**ASA** のバージョン	**ASA** モデル						
			5506-X シリーズ	**5508-X** **5516-X**	**5512-X**	**5515-X**	**5525-X** **5545-X** **5555-X**	**5585-X**（以下の **SSP** についての注記を参照してください）	**ISA 3000**
6.7.x	ASDM 7.15(1)	ASA 9.15(x) ASA 9.14(x) ASA 9.13(x) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)	—	**YES**	—	—	—	—	**YES**

ASA FirePOWER のバージョン	ASDM のバージョン（ローカル管理用）	ASA のバージョン	ASA モデル						
			5506-X シリーズ	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（以下の SSP についての注記を参照してください）	ISA 3000
6.6.x	ASDM 7.14(1)	ASA 9.15(x)（5525-X、5545-X、5555-X 以外） ASA 9.14(x) ASA 9.13(x) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)	—	**YES**	—	—	**YES**	—	**YES**
6.5.0	ASDM 7.13(1)	ASA 9.15(x)（5525-X、5545-X、5555-X 以外） ASA 9.14(x) ASA 9.13(x) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)	—	**YES**	—	—	**YES**	—	**YES**

ASA FirePOWER のバージョン	ASDM のバージョン（ローカル管理用）	ASA のバージョン	ASA モデル						
			5506-X シリーズ	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（以下の SSP についての注記を参照してください）	ISA 3000
6.4.0	ASDM 7.12(1)	ASA 9.15(x)（5515-X、5525-X、5545-X、5555-X、5585-X 以外） ASA 9.14(x)（5515-X、5585-X 以外） ASA 9.13(x)（5515-X、5585-X 以外） ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)	—	**YES**	—	**YES**	**YES**	**YES**	**YES**

ASA FirePOWER のバージョン	ASDM のバージョン（ローカル管理用）	ASA のバージョン	ASA モデル						
			5506-X シリーズ	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（以下の SSP についての注記を参照してください）	ISA 3000
6.3.0	ASDM 7.10(1)	ASA 9.15(x)（5515-X、5525-X、5545-X、5555-X、5585-X 以外） ASA 9.14(x)（5515-X、5585-X 以外） ASA 9.13(x)（5515-X、5585-X 以外） ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)	—	**YES**	—	**YES**	**YES**	**YES**	**YES**

ASA FirePOWER のバージョン	ASDM のバージョン（ローカル管理用）	ASA のバージョン	ASA モデル						
			5506-X シリーズ	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（以下の SSP についての注記を参照してください）	ISA 3000
6.2.3	ASDM 7.9(2)	ASA 9.15(x)（5506-X、5512-X、5515-X、5525-X、5545-X、5555-X、5585-X 以外） ASA 9.14(x)（5506-X、5512-X、5515-X、5585-X 以外） ASA 9.13(x)（5506-X、5512-X、5515-X、5585-X 以外） ASA 9.12(x)（5506-X、5512-X 以外） ASA 9.10(x)（5506-x、5512-x 以外） ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)（5506-X 以外）	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—

ASA FirePOWER のバージョン	ASDM のバージョン（ローカル管理用）	ASA のバージョン	ASA モデル						
			5506-X シリーズ	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（以下の SSP についての注記を参照してください）	ISA 3000
6.2.2	ASDM 7.8(2)	ASA 9.15(x)（5506-X、5512-X、5515-X、5525-X、5545-X、5555-X、5585-X 以外） ASA 9.14(x)（5506-X、5512-X、5515-X、5585-X 以外） ASA 9.13(x)（5506-X、5512-X、5515-X、5585-X 以外） ASA 9.12(x)（5506-X、5512-X 以外） ASA 9.10(x)（5506-x、5512-x 以外） ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)（5506-X 以外）	YES	YES	YES	YES	YES	YES	—

ASA FirePOWER のバージョン	ASDM のバージョン（ローカル管理用）	ASA のバージョン	ASA モデル						
			5506-X シリーズ	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（以下の SSP についての注記を参照してください）	ISA 3000
6.2.0	ASDM 7.7(1)	ASA 9.15(x)（5506-X、5512-X、5515-X、5525-X、5545-X、5555-X、5585-X 以外） ASA 9.14(x)（5506-X、5512-X、5515-X、5585-X 以外） ASA 9.13(x)（5506-X、5512-X、5515-X、5585-X 以外） ASA 9.12(x)（5506-X、5512-X 以外） ASA 9.10(x)（5506-x、5512-x 以外） ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)（5506-X 以外）	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—

ASA FirePOWER のバージョン	ASDM のバージョン（ローカル管理用）	ASA のバージョン	ASA モデル						
			5506-X シリーズ	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（以下の SSP についての注記を参照してください）	ISA 3000
6.1.0	ASDM 7.6(2)	ASA 9.15(x)（5506-X、5512-X、5515-X、5525-X、5545-X、5555-X、5585-X 以外） ASA 9.14(x)（5506-X、5512-X、5515-X、5585-X 以外） ASA 9.13(x)（5506-X、5512-X、5515-X、5585-X 以外） ASA 9.12(x)（5506-X、5512-X 以外） ASA 9.10(x)（5506-x、5512-x 以外） ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3)（5506-X 以外）	YES	YES	YES	YES	YES	YES	—

ASA FirePOWER のバージョン	ASDM のバージョン（ローカル管理用）	ASA のバージョン	ASA モデル						
			5506-X シリーズ	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（以下の SSP についての注記を参照してください）	ISA 3000
6.0.1	ASDM 7.6(1)（ASDM では ASA 9.4(x) のサポートなし、FMC のみ）	ASA 9.6(x) ASA 9.5(1.5)、9.5(2)、9.5(3) ASA 9.4(x) CSCuv91730 を考慮して、9.4(2) 以降にアップグレードすることをお勧めします。	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—
6.0.0	ASDM 7.5(1.112)（ASDM では ASA 9.4(x) のサポートなし、FMC のみ）	ASA 9.6(x) ASA 9.5(1.5)、9.5(2)、9.5(3) ASA 9.4(x) CSCuv91730 を考慮して、9.4(2) 以降にアップグレードすることをお勧めします。	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—

ASA FirePOWER のバージョン	ASDM のバージョン（ローカル管理用）	ASA のバージョン	ASA モデル						
			5506-X シリーズ	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（以下の SSP についての注記を参照してください）	ISA 3000
5.4.1.7+	ASDM 7.5(1.112)（ASDM では ASA 9.4(x) のサポートなし、FMC のみ）	ASA 9.15(x)（5506-X、5512-X、5515-X、5525-X、5545-X、5555-X、5585-X 以外） ASA 9.14(x)（5506-X 以外） ASA 9.13(x)（5506-X 以外） ASA 9.12(x)（5506-X 以外） ASA 9.10(x)（5506-X 以外） ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2)、9.5(3) ASA 9.4(x) ASA 9.4(1.225)（ISA 3000 のみ） ASA 9.3(2)、9.3(3)（5508-X または 5516-X 以外） CSCuv91730 を考慮して、9.3(3.8) または 9.4(2) 以降にアップグレードすることをお勧めします。	**YES**	**YES**	**—**	—	—	—	**YES**

ASA FirePOWER のバージョン	ASDM のバージョン（ローカル管理用）	ASA のバージョン	ASA モデル						
			5506-X シリーズ	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（以下の SSP についての注記を参照してください）	ISA 3000
5.4.1	ASDM 7.3(3)	ASA 9.15(x)（5506-X 以外） ASA 9.14(x)（5506-X 以外） ASA 9.13(x)（5506-X 以外） ASA 9.12(x)（5506-X 以外） ASA 9.10(x)（5506-X 以外） ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(1.5)、9.5(2)、9.5(3) ASA 9.4(x) ASA 9.3(2)、9.3(3)（5506-X のみ） CSCuv91730 を考慮して、9.3(3.8) または 9.4(2) 以降にアップグレードすることをお勧めします。	**YES**	**YES**	—	—	—	—	—

ASA FirePOWER のバージョン	ASDM のバージョン（ローカル管理用）	ASA のバージョン	ASA モデル						
			5506-X シリーズ	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（以下の SSP についての注記を参照してください）	ISA 3000
5.4.0.2+	—	ASA 9.14(x)（5512-X、5515-X、5585-X 以外） ASA 9.13(x)（5512-X、5515-X、5585-X 以外） ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(1.5)、9.5(2)、9.5(3) ASA 9.4(x) ASA 9.3(2)、9.3(3) CSCuv91730 を考慮して、9.3(3.8) または 9.4(2) 以降にアップグレードすることをお勧めします。	—	—	YES	YES	YES	YES	—
5.4.0.1	—	ASA 9.2(2.4)、9.2(3)、9.2(4) CSCuv91730 を考慮して、9.2(4.5) 以降にアップグレードすることをお勧めします。	—	—	YES	YES	YES	YES	—

ASA FirePOWER のバージョン	ASDM のバージョン（ローカル管理用）	ASA のバージョン	ASA モデル						
			5506-X シリーズ	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X（以下の SSP についての注記を参照してください）	ISA 3000
5.3.1	—	ASA 9.2(2.4)、9.2(3)、9.2(4) CSCuv91730 を考慮して、9.2(4.5) 以降にアップグレードすることをお勧めします。	—	—	**YES**	**YES**	**YES**	**YES**	—

ASA 5585-X SSP の互換性

同一レベル SSP

ASA FirePOWER SSP-10、-20、-40、および -60

要件：スロット *1* にインストールし、スロット *0* に一致するレベルの *ASA SSP* をインストールする

混在レベル SSP

次の組み合わせのサポートは、バージョン 5.4.0.1 から開始されます。

- ASA SSP-10/ASA FirePOWER SSP-40
- ASA SSP-20/ASA FirePOWER SSP-60
- ASA SSP-40/ASA FirePOWER SSP-60

要件：スロット *0* で *ASA SSP*、スロット *1* で *ASA FirePOWER SSP*

（注） SSP40/60 の組み合わせはサポートされていないため、エラー メッセージが表示される可能性があります。このメッセージは無視できます。

FMC デバイスのバージョン互換性を維持できるか

Firepower Management Center では、その管理対象デバイスと同じまたはより新しいバージョンを実行する必要があります。これは、以下を意味します。

- より新しい FMC でより古いデバイスを管理できます。通常は、メジャーバージョンをいくつか遡ることができます。

  たとえば、バージョン 6.7.0 の FMC では、バージョン 6.3.0 のデバイスを管理できます。

- FMC よりも新しいバージョンのデバイスをアップグレードすることはできません。

  FMC をアップグレードする前に、アップグレードされた FMC が現在のデバイスを管理できることを確認します。たとえば、バージョン 6.7.1 の FMC では、バージョン 6.7.0 のデバイスを管理できますが、バージョン 6.7.2 のデバイスは管理できません。

以下に、FMC のバージョンとそれによって管理できるデバイスを示します。一番左の列で現在のバージョンを見つけて、その行でどのデバイスを管理できるか確認します。特定のメジャーバージョン内では、FMC は管理対象デバイスと同じまたはより新しいメンテナンス（3 桁目）リリースを実行している必要があります。

表 *6 : FMC* 管理機能：バージョン *6.2.3+*

FMC バージョン	管理可能：デバイスバージョン									
	6.7.x	**6.6.x**	**6.5.0**	**6.4.0**	**6.3.0**	**6.2.3**	**6.2.2**	**6.2.1**	**6.2.0**	**6.1.0**
6.7.x	**YES**	**YES**	**YES**	**YES**	**YES**	—	—	—	—	—
6.6.x	—	**YES**	**YES**	**YES**	**YES**	**YES**	—	—	—	—
6.5.0	—	—	**YES**	**YES**	**YES**	**YES**	—	—	—	—
6.4.0	—	—	—	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
6.3.0	—	—	—	—	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
6.2.3	—	—	—	—	—	**YES**	**YES**	**YES**	**YES**	**YES**

表 *7 : FMC* 管理機能：バージョン *5.4.0 ～ 6.2.2*

FMC バージョン	管理可能：デバイスバージョン							
	6.2.2	**6.2.1**	**6.2.0**	**6.1.0**	**6.0.1**	**6.0.0**	**5.4.1**	**5.4.0**
6.2.2	**YES**	**YES**	**YES**	**YES**	—	—	—	—
6.2.1	—	**YES**	**YES**	**YES**	—	—	—	—
6.2.0	—	—	**YES**	**YES**	—	—	—	—
6.1.0	—	—	—	**YES**	**YES**	**YES**	○ *	○ *
6.0.1	—	—	—	—	**YES**	**YES**	○ *	○ *
6.0.0	—	—	—	—	—	**YES**	○ *	○ *
5.4.1	—	—	—	—	—	—	**YES**	**YES**

FMC バージョン	管理可能：デバイスバージョン							
	6.2.2	**6.2.1**	**6.2.0**	**6.1.0**	**6.0.1**	**6.0.0**	**5.4.1**	**5.4.0**
5.4.0	—	—	—	—	—	—	—	**YES**

* バージョン 6.0、6.0.1、または 6.1 の FMC で管理するには、デバイスが少なくともバージョン 5.4.0.2/5.4.1.1 を実行している必要があります。

技術的には、パッチが適用されていない FMC で、パッチが適用されたデバイス（4 桁番号のリリース）を管理できます。ただし、この方法は避けることを強くお勧めします。常に展開全体を更新する必要があります。多くの場合、新機能の使用や問題解決の適用には、FMC とその管理対象デバイスの両方で最新リリースが必要になります。

Firepower 4100/9300 と ASA または FTD の互換性

次の表に ASA または FTD アプリケーションと FXOS および Firepower モデルの互換性を示します。

「（EoL）」が付加されているバージョンの FXOS は、ライフサイクルが終了（EoL）しているかサポートが終了しています。

（注） 以下に**太字**でリストされているバージョンは、特別に認定されたリリースです。シスコがこれらの組み合わの拡張テストを実施するため、これらのソフトウェアの組み合わせは可能な限り使用する必要があります。

（注） Firepower 1000 および 2100 シリーズ アプライアンスは、ASA と Firepower Threat Defense の統合イメージ バンドルに含まれる基盤となるオペレーティング システムとしてのみ FXOS を使用します。

表 *8 : ASA* または *FTD*、および *Firepower 4100/9300* の互換性

FXOS のバージョン	FirePOWER モデル	ASA のバージョン	FTD バージョン
2.9(1.131)	Firepower 4112	**9.15(1)** 9.14(1)	**6.7.0**（推奨） 6.6.0
	Firepower 4145 Firepower 4125 Firepower 4115	**9.15(1)**（推奨） 9.14(1) 9.13(1) 9.12(x)	**6.7.0**（推奨） 6.6.0 6.5.0 6.4.0
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.15(1)**（推奨） 9.14(1) 9.13(x) 9.12(x) 9.10(x) 9.9(x) 9.8(x)	**6.7.0**（推奨） 6.6.0 6.5.0 6.4.0 6.3.0
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS のバージョン	FirePOWER モデル	ASA のバージョン	FTD バージョン
2.8(1.105)+ （注） FXOS 2.8(1.125)+ には ASA 9.14(1.15) 以降が必要	Firepower 4112	**9.14(1)** （注） ASA 9.14(1.15)+ には FXOS 2.8(1.125) 以降が必要	**6.6.0**
	Firepower 4145 Firepower 4125 Firepower 4115	**9.14(1)**（推奨） 9.13(1) 9.12(x)	**6.6.0**（推奨） 6.5.0 6.4.0
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	（注） Firepower 9300 SM-56 には ASA 9.12(2) 以降が必要 （注） ASA 9.14(1.15)+ には FXOS 2.8(1.125) 以降が必要	
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.14(1)**（推奨） 9.13(x) 9.12(x) 9.10(x)	**6.6.0**（推奨） 6.5.0 6.4.0 6.3.0
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.9(x) 9.8(x) 9.6(4) （注） ASA 9.14(1.15)+ には FXOS 2.8(1.125) 以降が必要	6.2.3 6.2.0

FXOS のバージョン	FirePOWER モデル	ASA のバージョン	FTD バージョン
2.7(1.92)+	Firepower 4145 Firepower 4125 Firepower 4115	**9.13(1)**（推奨） 9.12(x) （注） Firepower 9300 SM-56 には ASA 9.12.2 以降が必要	**6.5.0**（推奨） 6.4.0
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.13(1)**（推奨） 9.12(x) 9.10(1) 9.9(x) 9.8(x) 9.6(4)	**6.5.0**（推奨） 6.4.0 6.3.0 6.2.3 6.2.2 6.2.0
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.6(1.157)+ （注） ASA 9.12+ および FTD 6.4+ では、同じ Firepower 9300 シャーシ内の別のモジュールで実行できるようになりました。	Firepower 4145 Firepower 4125 Firepower 4115	**9.12(x)** （注） Firepower 9300 SM-56 には ASA 9.12.2 以降が必要	**6.4.0**
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12(x)**（推奨） 9.10(1) 9.9(x) 9.8(x) 9.6(4) （注） 9.7(x) はサポート対象外	**6.4.0**（推奨） 6.3.0 6.2.3 6.2.2 6.2.0 6.1.0
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS のバージョン	FirePOWER モデル	ASA のバージョン	FTD バージョン
2.6(1.131)	Firepower 9300 SM-48 Firepower 9300 SM-40	**9.12(x)**	サポート対象外
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12(x)**（推奨） 9.10(1) 9.9(x) 9.8(x) 9.6(4) （注） 9.7(x) はサポート対象外	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.4(1.214)+ （注） ハードウェアバイパスには FXOS 2.4.1.238 が必要です。詳細については、『Cisco Firepower 4100/9300 FXOS Release Notes, 2.4(1)』の「Important Notes」のセクションを参照してください。	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.10(1)**（推奨） 9.9(x) 9.8(x) 9.6(3)、9.6(4) （注） 9.7(x) はサポート対象外	**6.3.0**（推奨） 6.2.3 6.2.2 6.2.0 6.1.0
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.4(1.101)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.10(1)**（推奨） 9.9(x) 9.8(x) 9.6(3)、9.6(4) （注） 9.7(x) はサポート対象外	サポート対象外
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS のバージョン	FirePOWER モデル	ASA のバージョン	FTD バージョン
2.3(1.73)+	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110 Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	**9.9(x)**（推奨） 9.8(x) 9.7(x) 9.6(3)、9.6(4) （注） FXOS 2.3(1.130) 以降を実行している場合、フローオフロードには 9.8(2.12) 以降が必要です。	**6.2.3**（推奨） （注） Firepower 6.2.3.16+ には FXOS 2.3.1.157+ が必要 6.2.2 6.2.0 6.1.0 （注） FXOS 2.3(1.130) 以降を実行している場合、フローオフロードには 6.2.2.2 以降が必要です。
2.3(1.66) 2.3(1.58) 2.3(1.56) （注） FXOS 2.3(1.56) は、Cisco.com で一時的に提供されていましたが、サポートされなくなりました。詳細については、『Cisco FXOS Release Notes, 2.3(1)』を参照してください。	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110 Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	**9.9(x)**（推奨） 9.8(x) 9.7(x) 9.6(3)、9.6(4) （注） FXOS 2.3(1.130) 以降を実行している場合、フローオフロードには 9.8(2.12) 以降が必要です。	**6.2.2**（推奨） 6.2.2 6.2.0 6.1.0 （注） FXOS 2.3(1.130) 以降を実行している場合、フローオフロードには 6.2.2.2 以降が必要です。
2.2(2)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110 Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	**9.8(x)** （推奨）	**6.2.2**（推奨） 6.2.0 （注） FXOS 2.2(2.91) 以降を実行している場合、フローオフロードには 6.2.2 以降が必要です。

FXOS のバージョン	FirePOWER モデル	ASA のバージョン	FTD バージョン
2.2(1)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.8(1)**（推奨） 9.7(x) （注） フロー オフロードには 9.7(1.15) 以降が必要です。	**6.2.0**（推奨） （注） フロー オフロードには 6.2.0.3 以降が必要です。
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.1(1)（EoL）	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.7(x)**（推奨） 9.6(2)、9.6(3)、9.6(4)	**6.2.0**（推奨） 6.1.0
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.0(1)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.6(2)、9.6(3)、9.6(4)**（推奨） 9.6(1)	**6.1.0**（推奨） 6.0.1
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
1.1(4)	Firepower 4140 Firepower 4120 Firepower 4110	**9.6(1)**	**6.0.1**（推奨）
	Firepower 9300 SM-36 Firepower 9300 SM-24	**9.6(1)**（推奨） 9.5(2)、9.5(3)	
1.1(3)	Firepower 9300 SM-36 Firepower 9300 SM-24	**9.5(2)、9.5(3)**（推奨） 9.4（2）	サポート対象外
1.1(2)	Firepower 9300 SM-36 Firepower 9300 SM-24	**9.4(2)**（推奨） 9.4(1)	サポート対象外

FXOS のバージョン	FirePOWER モデル	ASA のバージョン	FTD バージョン
1.1(1)（EOL）	Firepower 9300 SM-36 Firepower 9300 SM-24	**9.4(1)**（推奨）	サポート対象外

Radware DefensePro の互換性

次の表に、各 Firepower セキュリティアプライアンスおよび関連する論理デバイスでサポートされる Radware DefensePro バージョンを示します。

表 *9 : Radware DefensePro* の互換性

FXOS のバージョン	ASA	Firepower Threat Defense	Radware DefensePro	Firepower のモデル
1.1(4)	9.6(1)	未サポート	1.1(2.32 ～ 3)	9300
2.0(1)	9.6(1) 9.6(2) 9.6(3) 9.6(4)	未サポート	8.10.01.16-5	Firepower 9300 Firepower 4120 Firepower 4140 Firepower 4150
2.1(1)	9.6(2) 9.6(3) 9.6(4) 9.7(1)	未サポート	8.10.01.16-5	Firepower 9300 Firepower 4120 Firepower 4140 Firepower 4150
2.2(1)	9.7(1) 9.8(1)	6.2.0	8.10.01.17-2	Firepower 9300 Firepower 4110（Firepower Threat Defense のみ） Firepower 4120 Firepower 4140 Firepower 4150
2.2(2)	9.8(1) 9.8(2) 9.8(3)	6.2.0 6.2.2	8.10.01.17-2	Firepower 9300 Firepower 4110（Firepower Threat Defense のみ） Firepower 4120 Firepower 4140 Firepower 4150

FXOS のバージョン	ASA	Firepower Threat Defense	Radware DefensePro	Firepower のモデル
2.3(1)	9.9(1) 9.9(2)	6.2.2 6.2.3	8.13.01.09-2	Firepower 9300 Firepower 4110（Firepower Threat Defense のみ） Firepower 4120 Firepower 4140 Firepower 4150
2.4(1)	9.9(2) 9.10(1)	6.2.3 6.3	8.13.01.09-2	Firepower 9300 Firepower 4110 Firepower 4120 Firepower 4140 Firepower 4150
2.6(1)	9.12(1) 9.10(1)	6.4.0 6.3.0	8.13.01.09-3	Firepower 9300 Firepower 4110 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.7(1)	9.13(1)	6.5	8.13.01.09-3	Firepower 9300 Firepower 4110 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150

FXOS のバージョン	ASA	Firepower Threat Defense	Radware DefensePro	Firepower のモデル
2.8.1	9.14(1)	6.6.0	8.13.01.09-3	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.9.1	9.15(1)	6.7.0	8.13.01.09-3	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150

アップグレード パス

アップグレードするオペレーティング システムごとに、サポートされているアップグレードパスを確認します。場合によっては、最終バージョンにアップグレードする前に、中間アップグレードをインストールする必要があります。

ASA のアップグレードパス

現在のバージョンとモデルを表示するには、次のいずれかの方法を使用します。

- CLI：**show version** コマンドを使用します。
- ASDM：**[Home）][Device Dashboard][Device Information]** の順に選択します。

次の表で、お使いのバージョンのアップグレードパスを参照してください。バージョンによっては、新しいバージョンにアップグレードする前に、中間アップグレードが必要な場合があります。推奨バージョンは**太字**で示されています。

（注） ASA のセキュリティの問題と、各問題に対する修正を含むリリースについては、ASA Security Advisories を参照してください。

（注） ASA 9.14(x) は ASA 5525-X、5545-X、および 5555-X の最終バージョンです。

ASA 9.12(x) は ASA 5512-X、5515-X、5585-X、および ASASM 用の最終バージョン、

ASA 9.2(x) は ASA 5505 用の最終バージョン、

ASA 9.1(x) は ASA 5510、5520、5540、5550、および 5580 用の最終バージョンです。

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.14(x)	—	次のいずれかになります。 → **9.15(x)**
9.13(x)	—	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)**
9.12(x)	—	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)**
9.10(x)	—	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x)

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.9(x)	—	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x)
9.8(x)	—	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)**
9.7(x)	—	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)**

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.6(x)	—	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.5(x)	—	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.4(x)	—	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.3(x)	—	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.2(x)	—	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.1(2)、9.1(3)、9.1(4)、9.1(5)、9.1(6)、または 9.1(7.4)	—	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.1(1)	→ 9.1(2)	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
9.0(2)、9.0(3)、または 9.0(4)	—	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.0(1)	→ 9.0(4)	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.6(1)	→ 9.0(4)	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
8.5(1)	→ 9.0(4)	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.4(5+)	—	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4) → 9.0(4)

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
8.4(1) ～ 8.4(4)	→ 9.0(4)	→ **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.2(x) 以前	→ 9.0(4)	次のいずれかになります。 → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)

ASA FirePOWER ASDM によるアップグレード パス

次の表に、ASDM によって管理される ASA FirePOWER module のアップグレードパスを示します。 現在のバージョンから目的のバージョンに直接アップグレードできない場合は、指示に従ってアップグレード パスに中間バージョンを含める必要があります。

ASDM で**[Home]** > **[ASA FirePOWER Dashboard]** を選択すると、現在のバージョンが表示されます。

（注） ASA 5506-X シリーズおよび ASA 5512-X では、任意の Firepower バージョンで ASA 9.10(1)+ を実行している ASA FirePOWER モジュールはサポートされません。

ASA 5585-X シリーズおよび ASA 5515-X では、任意の Firepower バージョンで ASA 9.10(1)+ を実行している ASA FirePOWER モジュールはサポートされません。

ASA 5525-X、5545-X、および 5555-X は、任意の Firepower バージョンで ASA 9.15(1)+ を実行している ASA FirePOWER モジュールをサポートしていません。

（注） バージョン 6.0 にアップグレードするには、プレインストールパッケージが必要です。詳細については、『FireSIGHT System Release Notes Version 6.0.0 Preinstallation』を参照してください。

現在のバージョン	ターゲットバージョン
6.7.x	直接アップグレード先： → 6.7.x メンテナンスリリース以降
6.6.x ASA 5525-X、5545-X、および 5555-X の最後のサポート対象 Firepower バージョン。	直接アップグレード先（次のいずれか）： → 6.7.x → 6.6.x メンテナンスリリース以降
6.5.0	直接アップグレード先： → 6.7.x → 6.6.x
6.4.0 ASA 5585-x シリーズおよび ASA 5515-x で最後にサポートされる Firepower バージョン。	直接アップグレード先（次のいずれか）： → 6.7.x → 6.6.x → 6.5.0

現在のバージョン	ターゲットバージョン
6.3.0	直接アップグレード先（次のいずれか）： → 6.7.x → 6.6.x → 6.5.0 →6.4.0
6.2.3 ASA 5506-x シリーズおよび ASA 5512-x で最後にサポートされる Firepower バージョン。 CSCvu50400 のため、ASDM 搭載の ASA FirePOWER をバージョン 6.2.3.x から 6.6.0 へ直接アップグレードしないでください。アップグレードは成功しますが、重大なパフォーマンスの問題が発生するため、Cisco TAC に連絡して修正を依頼する必要があります。代わりに、中間リリースにアップグレードしてから、バージョン6.6.0にアップグレードする必要があります。	直接アップグレード先（次のいずれか）： → 6.5.0 →6.4.0 → 6.3.0
6.2.2	直接アップグレード先（次のいずれか）： →6.4.0 → 6.3.0 → 6.2.3
6.2.1 このプラットフォームではサポートされていません。	—
6.2.0	直接アップグレード先： →6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	直接アップグレード先： → 6.2.0

現在のバージョン	ターゲットバージョン
6.0.1	直接アップグレード先： → 6.1.0
6.0.0	直接アップグレード先： → 6.0.1
5.4.0.2 または 5.4.1.1	直接アップグレード先（次のいずれか）： → 6.0.0

Asa FirePOWER アップグレードパス：FMC 搭載アップグレードパス：ASA FirePOWER

次の表に、Firepower Management Center によって管理される ASA FirePOWER module のアップグレードパスを示します。

（注） ASA 5506-X シリーズおよび ASA 5512-X では、任意の Firepower バージョンで ASA 9.10(1)+ を実行している ASA FirePOWER モジュールはサポートされません。

ASA 5585-X シリーズおよび ASA 5515-X では、任意の Firepower バージョンで ASA 9.10(1)+ を実行している ASA FirePOWER モジュールはサポートされません。

ASA 5525-X、5545-X、および 5555-X は、任意の Firepower バージョンで ASA 9.15(1)+ を実行している ASA FirePOWER モジュールをサポートしていません。

（注） ASA FirePOWER をバージョン 6.0.0 にアップグレードするには、プレインストールパッケージが必要です。詳細については、『FireSIGHT System Release Notes Version 6.0.0 Preinstallation』を参照してください。

左側の列で現在の Firepower のバージョンを確認します。右側の列に記載されているバージョンに直接アップグレードできます。現在のバージョンから目的のバージョンに直接アップグレードできない場合は、指示に従ってアップグレードパスに中間バージョンを含める必要があります。

表 *10 :* 直接アップグレード：*FMC* を搭載した *ASA FirePOWER*

現在のバージョン	ターゲットバージョン
6.7.0 6.7.x（メンテナンスリリース）	直接アップグレード先： → 6.7.x メンテナンスリリース以降

現在のバージョン	ターゲットバージョン
6.6.0 6.6.x（メンテナンスリリース） ASA 5525-X、5545-X、および 5555-X の最後の Firepower サポート。	直接アップグレード先（次のいずれか）： → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.x メンテナンスリリース以降
6.5.0	直接アップグレード先（次のいずれか）： → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.0 または 6.6.x メンテナンスリリース
6.4.0 ASA 5585-X シリーズおよび ASA 5515-X の最後の Firepower サポート。	直接アップグレード先（次のいずれか）： → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.0 または 6.6.x メンテナンスリリース → 6.5.0
6.3.0	直接アップグレード先（次のいずれか）： → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.0 または 6.6.x メンテナンスリリース → 6.5.0 →6.4.0
6.2.3 ASA 5506-x シリーズおよび ASA 5512-x の最後の Firepower サポート。	直接アップグレード先（次のいずれか）： → 6.6.0 または 6.6.x メンテナンスリリース → 6.5.0 →6.4.0 → 6.3.0
6.2.2	直接アップグレード先（次のいずれか）： →6.4.0 → 6.3.0
6.2.0	直接アップグレード先（次のいずれか）： →6.4.0 → 6.3.0 → 6.2.3 → 6.2.2

現在のバージョン	ターゲットバージョン
6.1.0	直接アップグレード先（次のいずれか）： →6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	直接アップグレード先： → 6.1.0
6.0.0	直接アップグレード先： → 6.0.1
5.4.0.2 または 5.4.1.1	直接アップグレード先： → 6.0.0

アップグレードパス：Firepower Management Center

次の表に Firepower Management Center（FMCv を含む）のアップグレードパスを示します。

（注） FMC をバージョン 6.0.0 およびバージョン 6.0.1 にアップグレードするには、プレインストールパッケージが必要です。

左側の列で現在の Firepower のバージョンを確認します。右側の列に記載されているバージョンに直接アップグレードできます。現在のバージョンから目的のバージョンに直接アップグレードできない場合は、指示に従ってアップグレードパスに中間バージョンを含める必要があります。

表 *11 : FMC* の直接アップグレード

現在のバージョン	ターゲットバージョン
6.7.0 6.7.x（メンテナンスリリース）	直接アップグレード先： → 6.7.x メンテナンスリリース以降
6.6.0 6.6.x（メンテナンスリリース） FMC 2000 および 4000 の最後のサポート。	直接アップグレード先（次のいずれか）： → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.x メンテナンスリリース以降

現在のバージョン	ターゲットバージョン
6.5.0	直接アップグレード先（次のいずれか）： → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.0 または 6.6.x メンテナンスリリース
6.4.0 FMC 750、1500、および 3500 の最後のサポート。	直接アップグレード先（次のいずれか）： → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.0 または 6.6.x メンテナンスリリース → 6.5.0
6.3.0	直接アップグレード先（次のいずれか）： → 6.7.0 または 6.7.x メンテナンスリリース → 6.6.0 または 6.6.x メンテナンスリリース → 6.5.0
6.2.3	直接アップグレード先（次のいずれか）： → 6.6.0 または 6.6.x メンテナンスリリース → 6.5.0 →6.4.0 → 6.3.0
6.2.2	直接アップグレード先（次のいずれか）： →6.4.0 → 6.3.0 → 6.2.3
6.2.1	直接アップグレード先（次のいずれか）： →6.4.0 → 6.3.0 → 6.2.3 → 6.2.2

現在のバージョン	ターゲットバージョン
6.2.0	直接アップグレード先（次のいずれか）： →6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	直接アップグレード先（次のいずれか）： →6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	直接アップグレード先： → 6.1.0
6.0.0	直接アップグレード先： → 6.0.1
5.4.1.1	直接アップグレード先： → 6.0.0

アップグレードパス：Firepower 4100/9300 シャーシ上の FXOS

現在のバージョンとモデルを表示するには、次のいずれかの方法を使用します。

- FirePOWER シャーシマネージャ：[Overview] を選択し、上部にある [Model] フィールドと [Version] を確認します。
- CLI：バージョンについては、**show version** コマンドを使用し、「Package-Vers:」フィールドを確認します。モデルについては、**scope chassis 1** を入力し、次に **show inventory** を入力します。

ダウングレードについての注記

FXOS イメージのダウングレードは公式にはサポートされていません。シスコがサポートする唯一の FXOS のイメージバージョンのダウングレード方法は、デバイスの完全な再イメージ化を実行することです。

2.3 以降へのアップグレード

バージョン 2.3 以降の Firepower 4100/9300 シャーシ のアップグレード パスについては、次の表を参照してください。バージョン 2.3 以前の場合、現在のバージョンが 2.0 から始まるバージョン以降であれば、ターゲット バージョンに直接アップグレードできます。

また、インストール済みの論理デバイス用のアプリケーション バージョンをアップグレードする必要がある場合もあります。FXOS のアップグレード後、論理デバイスのアップグレードパスを確認し、必要な暫定アップグレードを実行します。また、暫定（必要な場合）およびターゲットの FXOS リリースでサポートされているアプリケーション バージョンについて、十分注意してください（Firepower 4100/9300 と ASA または FTD の互換性 （24 ページ） を参照）。

表 *12 : 2.3* 以降へのアップグレード

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
2.8(1.x)	—	→ 2.9(1.x)
2.7(1.x)	—	次のいずれかになります。 → 2.9(1.x) → 2.8(1.x)
2.6(1.x)	—	次のいずれかになります。 → 2.9(1.x) → 2.8(1.x) → 2.7(1.x)
2.4(1.x)	—	次のいずれかになります。 → 2.9(1.x) → 2.8(1.x) → 2.7(1.x) → 2.6(1.x)
2.3(1.x)	—	次のいずれかになります。 → 2.9(1.x) → 2.8(1.x) → 2.7(1.x) → 2.6(1.x) → 2.4(1.x)

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
2.2(2.x)	—	次のいずれかになります。 → 2.9(1.x) → 2.8(1.x) → 2.7(1.x) → 2.6(1.x) → 2.4(1.x) → 2.3(1.x)

2.2 以前へのアップグレード

Firepower 4100/9300 シャーシ のバージョン 2.2 までのアップグレード パスについては、次の表を参照してください。バージョン 2.2 以前の場合、すべて現在のバージョンとターゲット バージョンの間の中間バージョンにアップグレードする必要があります。

また、インストール済みの論理デバイス用のアプリケーションバージョンをアップグレードする必要がある場合もあります。各 FXOS リリースでサポートされているアプリケーション バージョンに十分注意してください（Firepower 4100/9300 と ASA または FTD の互換性 （24 ページ）を参照）。次に論理デバイスに必要な暫定アップグレードを実行します。

たとえば、FXOS 1.1(4) を ASA とともに 2.2(2) にアップグレードする場合は、次のアップグレードを順番に実行します。

1. FXOS：1.1(4) から 2.0(1) へのアップグレード。
2. FXOS：2.0(1) から 2.1(1) へのアップグレード。
3. ASA：9.6(1) から 9.7(1) へのアップグレード。
4. FXOS：2.1(1) から 2.2(1) へのアップグレード。
5. FXOS：2.2(1) から 2.2(2) へのアップグレード。
6. ASA：9.7(1) から 9.8(1) へのアップグレード。

表 *13 : 2.2* 以前へのアップグレード

現在のバージョン	アップグレード パス			
2.2(1.x)	→ 2.2(2.17)			
2.1(1.x)	→ 2.2(1.63)	→ 2.2(2.17)		
2.0(1.x)	→ 2.1(1.64)	→ 2.2(1.63)	→ 2.2(2.17)	
1.1(4.x)	→ 2.0(1.135)	→ 2.1(1.64)	→ 2.2(1.63)	→ 2.2(2.17)

Cisco.com からのソフトウェアのダウンロード

アップグレードを開始する前に Cisco.com からすべてのソフトウェア パッケージをダウンロードしてください。オペレーティング システムに応じて、また CLI または GUI を使用しているかどうかによって、イメージをサーバ上または管理コンピュータ上に配置する必要があります。サポートされているファイルの保存場所の詳細については、各インストール手順を参照してください。

（注） Cisco.com のログインおよびシスコ サービス契約が必要です。

ASA ソフトウェアのダウンロード

ASDM アップグレード ウィザードを使用している場合は、ソフトウェアを事前にダウンロードする必要はありません。フェールオーバーアップグレードなど手動でのアップグレードの場合は、ローカル コンピュータにイメージをダウンロードします。

CLI のアップグレードでは、TFTP、HTTP、FTP を含む、多くのタイプのサーバにソフトウェアを配置することができます。『ASA コマンド リファレンス』の **copy** コマンドを参照してください。

ASA ソフトウェアは Cisco.com からダウンロードできます。この表には、ASA パッケージについての命名規則と情報が含まれています。

ASA モデル	ダウンロードの場所	パッケージ
ASA 5506-X、ASA 5508-X、および ASA 5516-X	http://www.cisco.com/go/asa-firepower-sw	
	ASA ソフトウェア 使用しているモデル > [Adaptive Security Appliance (ASA) Software] > バージョンの順に選択します。	ASA ソフトウェアのファイルには asa962-**lfbff-k8.SPA** のような名前が付いています。
	ASDM ソフトウェア 使用しているモデル > [Adaptive Security Appliance (ASA) Device Manager] > バージョンの順に選択します。	ASDM ソフトウェアのファイルには asdm-762**.bin** のような名前が付いています。
	REST API ソフトウェア 使用しているモデル > [Adaptive Security Appliance REST API Plugin] > バージョンの順に選択します。	API ソフトウェアのファイルには asa-restapi-132-**lfbff-k8.SPA** のような名前が付いています。REST API をインストールするには、『API クイック スタート ガイド』http://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.htmlを参照してください
	ROMmon ソフトウェア ご使用のモデル > [ASA Rommon Software] > バージョンの順に選択します。	ROMMON ソフトウェアのファイルには asa5500-firmware-1108**.SPA** のような名前が付いています。

ASA モデル	ダウンロードの場所	パッケージ
ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X	http://www.cisco.com/go/asa-software	
	ASA ソフトウェア 使用しているモデル > [Software on Chassis] > [Adaptive Security Appliance (ASA) Software] > バージョンの順に選択します。	ASA ソフトウェアのファイルには asa962-**smp-k8.bin** のような名前が付いています。
	ASDM ソフトウェア 使用しているモデル > [Software on Chassis] > [Adaptive Security Appliance (ASA) Device Manager] > バージョンの順に選択します。	ASDM ソフトウェアのファイルには asdm-762**.bin** のような名前が付いています。
	REST API ソフトウェア 使用しているモデル > [Software on Chassis] > [Adaptive Security Appliance REST API Plugin] > バージョンの順に選択します。	API ソフトウェアのファイルには asa-restapi-132-**lfbff-k8.SPA** のような名前が付いています。REST API をインストールするには、『API クイック スタート ガイド』http://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.htmlを参照してください
	Cisco Application Policy Infrastructure Controller（APIC）の ASA デバイス パッケージ 使用しているモデル > [Software on Chassis] > [ASA for Application Centric Infrastructure (ACI) Device Packages] > バージョンの順に選択します。	APIC 1.2(7) 以降では、ファブリック挿入によるポリシー オーケストレーションまたはファブリック挿入のみのパッケージを選択します。デバイス ソフトウェアのファイルには asa-device-pkg-1.2.7.10**.zip** のような名前が付いています。ASA デバイス パッケージをインストールするには、『Cisco APIC Layer 4 to Layer 7 Services Deployment Guide』http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.htmlの「Importing a Device Package」の章を参照してください。

ASA モデル	ダウンロードの場所	パッケージ
ASA 5585-X	http://www.cisco.com/go/asa-software	
	ASA ソフトウェア 使用しているモデル > [Software on Chassis] > [Adaptive Security Appliance (ASA) Software] > バージョンの順に選択します。	ASA ソフトウェアのファイルには asa962-**smp-k8.bin** のような名前が付いています。
	ASDM ソフトウェア 使用しているモデル > [Software on Chassis] > [Adaptive Security Appliance (ASA) Device Manager] > バージョンの順に選択します。	ASDM ソフトウェアのファイルには asdm-762**.bin** のような名前が付いています。
	REST API ソフトウェア 使用しているモデル > [Software on Chassis] > [Adaptive Security Appliance REST API Plugin] > バージョンの順に選択します。	API ソフトウェアのファイルには asa-restapi-132-**lfbff-k8.SPA** のような名前が付いています。REST API をインストールするには、『API クイックスタート ガイド』http://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.htmlを参照してください。
	Cisco Application Policy Infrastructure Controller（APIC）の ASA デバイス パッケージ 使用しているモデル > [Software on Chassis] > [ASA for Application Centric Infrastructure (ACI) Device Packages] > バージョンの順に選択します。	APIC 1.2(7) 以降では、ファブリック挿入によるポリシー オーケストレーションまたはファブリック挿入のみのパッケージを選択します。デバイス ソフトウェアのファイルには asa-device-pkg-1.2.7.10**.zip** のような名前が付いています。ASA デバイス パッケージをインストールするには、『Cisco APIC Layer 4 to Layer 7 Services Deployment Guide』http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.htmlの「Importing a Device Package」の章を参照してください。

ASA モデル	ダウンロードの場所	パッケージ
ASAv	http://www.cisco.com/go/asav-software	
	ASA ソフトウェア（アップグレード） [Adaptive Security Appliance (ASA) Software] > バージョンの順に選択します。	ASAv アップグレード ファイルには、asa962-**smp-k8.bin** のような名前が付いています。すべてのスーパバイザにこのアップグレード ファイルを使用します。**注**：.zip（VMware）、.vhdx（Hyper-V）、および .qcow2（KVM）ファイルは初期展開専用です。Amazon Web Services および Microsoft Azure は、展開イメージを直接提供します。
	ASDM ソフトウェア（アップグレード） [Adaptive Security Appliance (ASA) Device Manager] > バージョンの順に選択します。	ASDM ソフトウェアのファイルには asdm-762**.bin** のような名前が付いています。
	REST API ソフトウェア [Adaptive Security Appliance REST API Plugin] > バージョンの順に選択します。	API ソフトウェアのファイルには asa-restapi-132-**lfbff-k8.SPA** のような名前が付いています。REST API をインストールするには、『API クイックスタート ガイド』http://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html を参照してください。
	Cisco Application Policy Infrastructure Controller（APIC）の ASA デバイス パッケージ [ASA for Application Centric Infrastructure (ACI) Device Packages] > バージョンの順に選択します。	APIC 1.2(7) 以降では、ファブリック挿入によるポリシー オーケストレーションまたはファブリック挿入のみのパッケージを選択します。デバイス ソフトウェアのファイルには asa-device-pkg-1.2.7.10**.zip** のような名前が付いています。ASA デバイス パッケージをインストールするには、『Cisco APIC Layer 4 to Layer 7 Services Deployment Guide』http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html の「Importing a Device Package」の章を参照してください。

ASA モデル	ダウンロードの場所	パッケージ
Firepower 1010、Firepower 1120、Firepower 1140、および Firepower 1150	http://www.cisco.com/go/asa-firepower-sw	
	ASA、ASDM、および FXOS ソフトウェア 使用しているモデル > [Adaptive Security Appliance (ASA) Software] > バージョンの順に選択します。	ASA パッケージには、ASA、ASDM、および FXOS ソフトウェアが含まれています。ASA パッケージには、cisco-asa-fp1k.9.13.1.**SPA** のような名前が付いています。
	ASDM ソフトウェア（アップグレード） 使用しているモデル > [Adaptive Security Appliance (ASA) Device Manager] > バージョンの順に選択します。	現在の ASDM または ASA CLI を使用して、以降のバージョンの ASDM にアップグレードするには、このイメージを使用します。ASDM ソフトウェアのファイルには asdm-7131.**bin** のような名前が付いています。 （注） ASA バンドルをアップグレードすると、同じ名前（**asdm.bin**）であるため、バンドル内の ASDM イメージが ASA 上の前の ASDM バンドル イメージに置き換わります。ただし、アップロードした別の ASDM イメージ（たとえば **asdm-7131.bin**）を手動で選択すると、バンドル アップグレード後も引き続き同じイメージが使用されます。互換性のある ASDM バージョンを実行していることを確認するには、バンドルをアップグレードする前に ASDM をアップグレードするか、または ASA バンドルをアップグレードする直前に、バンドルされた ASDM イメージ（**asdm.bin**）を使用するように ASA を再設定する必要があります。

ASA モデル	ダウンロードの場所	パッケージ
Firepower 2110、Firepower 2120、Firepower 2130、Firepower 2140	http://www.cisco.com/go/asa-firepower-sw	
	ASA、ASDM、および FXOS ソフトウェア 使用しているモデル > [Adaptive Security Appliance (ASA) Software] > バージョンの順に選択します。	ASA パッケージには、ASA、ASDM、および FXOS ソフトウェアが含まれています。ASA パッケージには、cisco-asa-fp2k.9.8.2.**SPA** のようなファイル名が付いています。
	ASDM ソフトウェア（アップグレード） 使用しているモデル > [Adaptive Security Appliance (ASA) Device Manager] > バージョンの順に選択します。	現在の ASDM または ASA CLI を使用して、以降のバージョンの ASDM にアップグレードするには、このイメージを使用します。ASDM ソフトウェアのファイルには asdm-782.**bin** のような名前が付いています。 （注） ASA バンドルをアップグレードすると、同じ名前（**asdm.bin**）であるため、バンドル内の ASDM イメージが ASA 上の前の ASDM バンドル イメージに置き換わります。ただし、アップロードした別の ASDM イメージ（たとえば **asdm-782.bin**）を手動で選択すると、バンドル アップグレード後も引き続き同じイメージが使用されます。互換性のある ASDM バージョンを実行していることを確認するには、バンドルをアップグレードする前に ASDM をアップグレードするか、または ASA バンドルをアップグレードする直前に、バンドルされた ASDM イメージ（**asdm.bin**）を使用するように ASA を再設定する必要があります。

ASA モデル	ダウンロードの場所	パッケージ
Firepower 4110、Firepower 4112、Firepower 4115、Firepower 4120、Firepower 4125、Firepower 4140、Firepower 4145、Firepower 4150 の ASA	http://www.cisco.com/go/firepower4100-software	
	ASA と ASDM のソフトウェア 使用しているモデル > [Adaptive Security Appliance (ASA) Software] > バージョンの順に選択します。	ASA パッケージには、ASA と ASDM の両方が含まれます。ASA パッケージのファイルには cisco-asa.9.6.2**.SPA.csp** のような名前が付いています。
	ASDM ソフトウェア（アップグレード） 使用しているモデル > [Adaptive Security Appliance (ASA) Device Manager] > バージョンの順に選択します。	現在の ASDM または ASA CLI を使用して、以降のバージョンの ASDM にアップグレードするには、このイメージを使用します。ASDM ソフトウェアのファイルには asdm-762**.bin** のような名前が付いています。 （注） FXOS で ASA バンドルをアップグレードすると、同じ名前（**asdm.bin**）であるため、バンドル内の ASDM イメージが ASA 上の前の ASDM バンドル イメージに置き換わります。ただし、アップロードした別の ASDM イメージ（たとえば **asdm-782.bin**）を手動で選択すると、バンドル アップグレード後も引き続き同じイメージが使用されます。互換性のある ASDM バージョンを実行していることを確認するには、バンドルをアップグレードする前に ASDM をアップグレードするか、または ASA バンドルをアップグレードする直前に、バンドルされた ASDM イメージ（**asdm.bin**）を使用するように ASA を再設定する必要があります。
	REST API ソフトウェア 使用しているモデル > [Adaptive Security Appliance REST API Plugin] > バージョンの順に選択します。	API ソフトウェアのファイルには asa-restapi-132-**lfbff-k8.SPA** のような名前が付いています。REST API をインストールするには、『API クイックスタート ガイド』http://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.htmlを参照してください。

ASA モデル	ダウンロードの場所	パッケージ
Firepower 9300 の ASA	http://www.cisco.com/go/firepower9300-software	
	ASA と ASDM のソフトウェア [Adaptive Security Appliance (ASA) Software] > バージョンの順に選択します。	ASA パッケージには、ASA と ASDM の両方が含まれます。ASA パッケージのファイルには cisco-asa.9.6.2.**SPA.csp** のような名前が付いています。
	ASDM ソフトウェア（アップグレード） [Adaptive Security Appliance (ASA) Device Manager] > バージョンの順に選択します。	現在の ASDM または ASA CLI を使用して、以降のバージョンの ASDM にアップグレードするには、このイメージを使用します。ASDM ソフトウェアのファイルには asdm-762.**bin** のような名前が付いています。 （注） FXOS で ASA バンドルをアップグレードすると、同じ名前（**asdm.bin**）であるため、バンドル内の ASDM イメージが ASA 上の前の ASDM バンドル イメージに置き換わります。ただし、アップロードした別の ASDM イメージ（たとえば **asdm-782.bin**）を手動で選択すると、バンドル アップグレード後も引き続き同じイメージが使用されます。互換性のある ASDM バージョンを実行していることを確認するには、バンドルをアップグレードする前に ASDM をアップグレードするか、または ASA バンドルをアップグレードする直前に、バンドルされた ASDM イメージ（**asdm.bin**）を使用するように ASA を再設定する必要があります。
	REST API ソフトウェア [Adaptive Security Appliance REST API Plugin] > バージョンの順に選択します。	API ソフトウェアのファイルには asa-restapi-132-**lfbff-k8.SPA** のような名前が付いています。REST API をインストールするには、『API クイックスタート ガイド』http://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html を参照してください。

ASA モデル	ダウンロードの場所	パッケージ
ASA サービス モジュール	**ASA ソフトウェア** http://www.cisco.com/go/asasm-software ご使用のバージョンを選択します。	ASA ソフトウェアのファイルには asa962-**smp-k8.bin** のような名前が付いています。
	ASDM ソフトウェア http://www.cisco.com/go/asdm-software [Adaptive Security Appliance (ASA) Device Manager] > バージョンの順に選択します。	ASDM ソフトウェアのファイルには asdm-762**.bin** のような名前が付いています。
ISA 3000	http://www.cisco.com/go/isa3000-software	
	ASA ソフトウェア 使用しているモデル > [Adaptive Security Appliance (ASA) Software] > バージョンの順に選択します。	ASA ソフトウェアのファイルには asa962-**lfbff-k8.SPA** のような名前が付いています。
	ASDM ソフトウェア 使用しているモデル > [Adaptive Security Appliance (ASA) Device Manager] > バージョンの順に選択します。	ASDM ソフトウェアのファイルには asdm-762**.bin** のような名前が付いています。
	REST API ソフトウェア 使用しているモデル > [Adaptive Security Appliance REST API Plugin] > バージョンの順に選択します。	API ソフトウェアのファイルには asa-restapi-132-**lfbff-k8.SPA** のような名前が付いています。REST API をインストールするには、『API クイックスタート ガイド』http://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.htmlを参照してください。

ASA FirePOWER ソフトウェアのダウンロード

ASDM を使用して ASA FirePOWER モジュールを管理する場合は、Cisco.com からソフトウェアをダウンロードします。

Firepower Management Center ソフトウェアを使用して ASA FirePOWER モジュールを管理する場合、次のいずれかの方法でソフトウェアをダウンロードできます。

- マイナーリリース（パッチやホットフィックス）の場合、**[System]** > **[Updates]** ページの Firepower Management Center の [Download Updates] 機能を使用します。Firepower Management Center と現在管理しているデバイス用のすべてのマイナーアップグレードがダウンロードされます。
- メジャー リリースの場合、Cisco.com からソフトウェアをダウンロードします。

この表には、Cisco.com 上の ASA FirePOWER ソフトウェアについての命名規則と情報が含まれています。

ASA モデル	ダウンロードの場所	パッケージ
ASA 5506-X、ASA 5508-X、および ASA 5516-X	http://www.cisco.com/go/asa-firepower-sw 使用しているモデル > [FirePOWER Services Software for ASA] > バージョンの順に選択します。	• **プレインストール ソフトウェア**：プレインストール ファイル（一部のアップグレード用）には Cisco_Network_Sensor_6.1.0_**Pre-install**-6.0.1.999-32**.sh** のような名前が付いています。 • **アップグレード ソフトウェア**：アップグレード ファイルには Cisco_Network_Sensor_**Upgrade**-6.2.0-362**.sh** のような名前が付いています。 • **ホットフィックス ソフトウェア**：ホットフィックス ファイルには Cisco_Network_Sensor_**Hotfix**_AF-6.1.0.2-1**.sh** のような名前が付いています。 • **ブート イメージ**：ブート イメージはイメージの再作成にのみ使用され、asasfr-5500x-**boot**-6.1.0-330**.img** のようなファイル名が付いています。 • **システム ソフトウェア インストール パッケージ**：システム ソフトウェア インストール パッケージはイメージの再作成にのみ使用され、asasfr-**sys**-6.1.0-330**.pkg** のようなファイル名が付いています。 • **パッチ ファイル**：パッチ ファイルには Cisco_Network_Sensor_**Patch**-6.1.0.1-53**.sh** のような名前が付いています。

ASA モデル	ダウンロードの場所	パッケージ
ASA 5512-X ～ ASA 5555-X	http://www.cisco.com/go/asa-firepower-sw 使用しているモデル > [FirePOWER Services Software for ASA] > バージョンの順に選択します。	• **プレインストール ソフトウェア**：プレインストール ファイル（一部のアップグレード用）には Cisco_Network_Sensor_6.1.0_**Pre-install**-6.0.1.999-32**.sh** のような名前が付いています。 • **アップグレード ソフトウェア**：アップグレード ファイルには Cisco_Network_Sensor_**Upgrade**-6.2.0-362**.sh** のような名前が付いています。 • **ホットフィックス ソフトウェア**：ホットフィックス ファイルには Cisco_Network_Sensor_**Hotfix**_AF-6.1.0.2-1**.sh** のような名前が付いています。 • **ブート イメージ**：ブート イメージはイメージの再作成にのみ使用され、asasfr-5500x-**boot**-6.1.0-330**.img** のようなファイル名が付いています。 • **システム ソフトウェア インストール パッケージ**：システム ソフトウェア インストール パッケージはイメージの再作成にのみ使用され、asasfr-**sys**-6.1.0-330**.pkg** のようなファイル名が付いています。 • **パッチ ファイル**：パッチ ファイルには Cisco_Network_Sensor_**Patch**-6.1.0.1-53**.sh** のような名前が付いています。

ASA モデル	ダウンロードの場所	パッケージ
ASA 5585-X	http://www.cisco.com/go/asa-firepower-sw ご使用のモデル>バージョン を選択します。	• **プレインストール ソフトウェア**：プレインストール ファイル（一部のアップグレード用）には Cisco_Network_Sensor_6.1.0_**Pre-install**-6.0.1.999-32**.sh** のような名前が付いています。 • **アップグレード ソフトウェア**：アップグレード ファイルには Cisco_Network_Sensor_**Upgrade**-6.2.0-362**.sh** のような名前が付いています。 • **ホットフィックス ソフトウェア**：ホットフィックス ファイルには Cisco_Network_Sensor_**Hotfix**_AF-6.1.0.2-1**.sh** のような名前が付いています。 • **ブート イメージ**：ブート イメージはイメージの再作成にのみ使用され、asasfr-5500x-**boot**-6.1.0-330**.img** のようなファイル名が付いています。 • **システム ソフトウェア インストール パッケージ**：システム ソフトウェア インストール パッケージはイメージの再作成にのみ使用され、asasfr-**sys**-6.1.0-330**.pkg** のようなファイル名が付いています。 • **パッチ ファイル**：パッチ ファイルには Cisco_Network_Sensor_**Patch**-6.1.0.1-53**.sh** のような名前が付いています。

ASA モデル	ダウンロードの場所	パッケージ
ISA 3000	http://www.cisco.com/go/isa3000-software 使用しているモデル > [FirePOWER Services Software for ASA] > バージョンの順に選択します。	• **ホットフィックス ソフトウェア**：ホットフィックス ファイルには Cisco_Network_Sensor_**Hotfix**_CX-5.4.1.9-1.**tar** のような名前が付いています。 • **ブートイメージ**：ブートイメージのファイルには asasfr-ISA-3000-**boot**-5.4.1-213.**img** のような名前が付いています。 • **システム ソフトウェア インストール パッケージ**：システム ソフトウェア インストール パッケージには asasfr-sys-5.4.1-213.**pkg** のような名前が付いています。 • **パッチ ファイル**：パッチ ファイルには Cisco_Network_Sensor_**Patch**-5.4.1.10-33.**sh** のような名前が付いています。

Firepower Management Center ソフトウェアのダウンロード

Firepower Management Center ソフトウェアは、シスコサポートおよびダウンロードサイトで入手できます。インターネットにアクセスできる FMC では、パッチおよびメンテナンスリリースについては、手動でのダウンロードが可能になってから約 2 週間後にシスコから直接ダウンロードできます。メジャーリリースについては、シスコから直接ダウンロードすることはできません。詳細については、Cisco Firepower Management Center Upgrade Guideを参照してください。

アップグレード パッケージの Firepower 4100/9300 シャーシFXOS

Firepower 4100/9300 シャーシ の FXOS アップグレード パッケージについては、次を参照してください：

- Firepower 4100 シリーズ： http://www.cisco.com/go/firepower4100-software
- Firepower 9300： http://www.cisco.com/go/firepower9300-software

使用しているモデル > [FirePOWER Extensible Operating System] > バージョンの順に選択します。

表 *14 : FXOS* アップグレードパッケージ

パッケージ タイプ	パッケージ名
FXOS イメージ	fxos-k9.バージョン**.SPA**
リカバリ（キックスタート）	fxos-k9-**キックスタート**.バージョン**.SPA**
リカバリ（マネージャ）	fxos-k9-**マネージャ**.バージョン**.SPA**
リカバリ（システム）	fxos-k9-**システム**.バージョン**.SPA**
MIB	fxos-**mibs**-fp9k-fp4k.バージョン**.zip**
ファームウェア： Firepower 4100 シリーズ	fxos-k9-fpr4k-**firmware**.バージョン**.SPA**
ファームウェア： Firepower 9300	fxos-k9-fpr9k-**firmware**.*version*.**SPA**

アップグレード前の重要なガイドライン

各オペレーティング システムのアップグレード ガイドライン、制約事項、および設定移行をチェックします。

ASA のアップグレード ガイドライン

アップグレードを行う前に、移行およびその他のガイドラインを確認してください。

バージョン固有のガイドラインおよび移行

現在お使いのバージョンにより、1 つまたは複数の設定の移行が必要になる場合があります。またアップグレード時に、最初のバージョンから最後のバージョンまですべてのバージョンの設定ガイドラインを考慮する必要があります。

9.15 のガイドライン

- Firepower 1010 では、無効な VLAN ID によって問題が発生する可能性があります。9.15(1) にアップグレードする前に、3968 ー 4047 の範囲内のスイッチポートに VLAN を使用していないことを確認してください。これらの ID は内部使用専用であり、9.15(1) には、これらの ID を使用していないことを確認するチェックが含まれます。たとえば、フェールオーバーペアのアップグレード後にこれらの ID が使用されていた場合、フェールオーバーペアは一時停止状態になります。詳細については、「CSCvw33057」を参照してください。
- ASA 9.15(1) での低セキュリティ暗号の削除：IKE および IPsecで使用される安全性の低い次の暗号のサポートが廃止されました。
  - Diffie-Hellman グループ：2 および 24

- 暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256、NULL、ESP-3DES、ESP-DES、ESP-MD5-HMAC
- ハッシュアルゴリズム：MD5

（注） 安全性の低い SSH 暗号と SSL 暗号はまだ廃止されていません。

ASA の以前のバージョンからバージョン 9.15(1) にアップグレードする前に、9.15(1) でサポートされている暗号を使用するように VPN 設定を更新する必要があります。そのようにしないと、古い設定が拒否されます。設定が拒否されると、コマンドに応じて次のいずれかのアクションが実行されます。

- コマンドはデフォルトの暗号を使用する。
- コマンドが削除される。

アップグレード前の設定の修正は、クラスタリングまたはフェールオーバーの展開で特に重要です。たとえば、セカンダリユニットが 9.15(1) にアップグレードされ、削除された暗号がプライマリからこのユニットに同期された場合、セカンダリユニットは設定を拒否します。この拒否により、クラスタへの参加の失敗などの予期しない動作が発生する可能性があります。

IKEv1：次のサブコマンドが削除されています。

- **crypto ikev1 policy** *priority*:
  - **hash md5**
  - **encryption 3des**
  - **encryption des**
  - **group 2**

IKEv2：次のサブコマンドが削除されています。

- **crypto ikev2 policy** *priority*:
  - **prf md5**
  - **integrity md5**
  - **group 2**
  - **group 24**
  - **encryption 3des**
  - **encryption des**
  - **encryption null**

IPsec：次のサブコマンドが削除されています。

- **crypto ipsec ikev1 transform-set *name* esp-3des esp-des esp-md5-hmac**
- **crypto ipsec ikev2 ipsec-proposal *name***
  - **protocol esp integrity md5**
  - **protocol esp encryption 3des aes-gmac aes-gmac- 192 aes-gmac -256 des**
- **crypto ipsec profile *name***
  - **set pfs group2 group24**

Crypto Map：次のサブコマンドが削除されています。

- **crypto map *name sequence* set pfs group2**
- **crypto map *name sequence* set pfs group24**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group2**

9.14 のガイドライン

- アプライアンスモードの Firepower 1000 および 2100 での ASDM Cisco.com アップグレードウィザードの失敗：ASDM Cisco.com アップグレードウィザードは、9.14 へのアップグレードには使用できません（[**Tools**] > [Check for ASA/ASDM Updates]）。ウィザードでは ASDM を 7.13 から 7.14 にアップグレードできますが、ASA イメージのアップグレードはグレー表示されます（CSCvt72183）。回避策として、次のいずれかの方法を使用してください。
  - ASA と ASDM の両方で **[Tools] > [Upgrade Software from Local Computer]** を使用します。9.14(1) バンドルの ASDM イメージ（7.14(1)）にも CSCvt72183 のバグがあることに注意してください。ウィザードを正しく機能させるには、より新しい 7.14(1.46) イメージをダウンロードする必要があります。
  - **[Tools] > [Check for ASA/ASDM Updates]** を使用して ASDM 7.14 にアップグレードします（バージョンは 7.14(1.46) になる）。次に、新しい ASDM を使用して ASA イメージをアップグレードします。**致命的なインストールエラー**が表示されることがあることに注意してください。この場合は、[**OK**] をクリックします。次に、**[Configuration] > [Device Management] > [System Image/Configuration] > [Boot Image/Configuration]** 画面で、ブートイメージを手動で設定する必要があります。設定を保存し、ASA をリロードします。

9.13 のガイドライン

- 9.13(1) 以降では ASAv に 2 GB のメモリが必要です（9.13(1) 以降の ASAv の最小メモリ要件は 2 GB）。現在の ASAv が 2 GB 未満のメモリで動作している場合は、以前のバージョンから 9.13(1) にアップグレードできません。アップグレードする前にメモリサイズを調整する必要があります。バージョン 9.13(1) でサポートされているリソース割り当て（vCPU とメモリ）については、ASAv のスタートアップガイドを参照してください。

- ローカル CA サーバは 9.13(1) で削除される：ASA がローカル CA サーバとして設定されている場合、デジタル証明書の発行、証明書失効リスト（CRL）の発行、および発行された証明書の安全な取り消しが可能です。この機能は古くなったため、**crypto ca server** コマンドは削除されています。

- 9.13(1) では、Diffie-Hellman Group 14 が **crypto map set pfs**、**crypto ipsec profile**、**crypto dynamic-map set pfs**、および **crypto map set ikev1 phase1-mode** を使用する IPsec PFS の **crypto ikev1 policy**、**ssl dh-group**、および **crypto ikev2 policy** の **group** コマンドのデフォルトになりました。以前のデフォルトの Diffie-Hellman グループは Group 2 でした。また、Diffie Hellman グループ 1 は、低セキュリティ IKE/IPsec 暗号であることが判明し、廃止されました。

  9.13 (1) 以前のリリースからアップグレードし、古いデフォルト（Diffie-Hellman Group 2）を使用する必要がある場合は、DH グループを **group 2** として手動で設定する必要があります。そうでない場合、トンネルはデフォルトで Group 14 に設定されます。group 2 は今後のリリースで削除されるため、できるだけ早く group 14 にトンネルを移動する必要があります。

- バイパス証明書の有効性チェックオプションの削除：CRL または OCSP サーバとの接続の問題による失効チェックをバイパスするオプションが削除されました。

  revocation-check：次のサブコマンドが削除されています。

  - **revocation-check crl none**
  - **revocation-check ocsp none**
  - **revocation-check crl ocsp none**
  - **revocation-check ocsp crl none**

  したがって、アップグレード後は、trailing none を無視することで、サポートされなくなった revocation-check コマンドは新しい動作に移行します。

- CRL 配布ポイントコマンドの削除：スタティック CDP URL 設定コマンド、つまり **crypto-ca-trustpoint crl** と **crl url** は関連する他のロジックとともに削除されました。

9.12 のガイドライン

- ASDM アップグレード ウィザード：内部的な変更により、このウィザードでは ASDM 7.10(1) 以降の使用のみがサポートされています。また、イメージの命名が変更されたため、ASA 9.10(1) 以降にアップグレードするには、ASDM 7.12(1) 以降を使用する必要があります。ASDM には ASA の以前のリリースと下位互換性があるため、実行している ASA バージョンを問わず、ASDM をアップグレードすることができます。

- 9.12(1) での SSH セキュリティの改善と新しいデフォルト設定：次の SSH セキュリティの改善点を参照してください。

  - SSH バージョン 1 はサポートされなくなりました。バージョン 2 のみがサポートされています。**ssh version 1** コマンドは **ssh version 2** に移行されます。

- Diffie-Hellman Group 14 SHA256 キー交換のサポート。この設定がデフォルト（**ssh key-exchange group dh-group14-sha256**）になりました。以前のデフォルトは Group 1 SHA1 でした。SSH クライアントが Diffie-Hellman Group 14 SHA256 をサポートしていることを確認してください。サポートしていない場合は、「Couldn't agree on a key exchange algorithm」などのエラーが表示されることがあります。たとえば、OpenSSH では Diffie-Hellman Group 14 SHA256 がサポートされています。
- HMAC-SHA256 整合性暗号のサポート。デフォルトは、高セキュリティの暗号セット（**ssh cipher integrity high** コマンドによって定義された hmac-sha1 および hmac-sha2-256）になりました。以前のデフォルトは中程度のセットでした。

- NULL-SHA TLSv1 暗号は廃止され、9.12(1) では削除されている：NULL-SHA は暗号化を提供せず、現在の脅威に対して安全とは見なされなくなったため、**tls-proxy** mode コマンド/オプションおよび **show ssl ciphers all** の出力に TLSv1 でサポートされている暗号を一覧表示すると削除されます。**ssl cipher tlsv1 all** コマンドと **ssl cipher tlsv1 custom NULL-SHA** コマンドも廃止され、削除されます。
- 9.12(1) ではデフォルトの trustpool が削除されている：PSB 要件、SEC-AUT-DEFROOT に準拠するため、「デフォルト」の信頼できる CA バンドルが ASA イメージから削除されています。その結果、 **crypto ca trustpool import default** コマンドと **crypto ca trustpool import clean default** コマンドも、その他の関連ロジックとともに削除されています。ただし、既存の展開では、これらのコマンドを使用して以前にインポートされた証明書はそのまま残ります。
- **ssl encryption** コマンドは 9.12(1) で削除されている：9.3(2) では、廃止が公表され、**ssl cipher** に置き換えられます。9.12(1) では、**ssl encryption** が削除され、サポートされなくなりました。

9.10 のガイドライン

- 内部的な変更により、ASDM アップグレードウィザードでは ASDM 7.10(1) 以降の使用のみがサポートされています。また、イメージの命名が変更されたため、ASA 9.10(1) 以降にアップグレードするには、ASDM 7.12(1) 以降を使用する必要がありますASDM にはASA の以前のリリースと下位互換性があるため、実行している ASA バージョンを問わず、ASDM をアップグレードすることができます。

9.9 のガイドライン

- 9.9(2) 以降での大規模な構成による ASA 5506-X のメモリの問題：9.9(2) 以降にアップグレードする場合、大規模な構成の一部がメモリ不足のため拒否され、「エラーが発生しました：ルールをインストールするためのメモリが不足しています（ERROR: Insufficient memory to install the rules）」のメッセージが表示される場合があります。これを回避する方法の 1 つに、**object-group-search access-control** コマンドを入力して、ACL のメモリ使用量を改善する方法があります。ただし、パフォーマンスに影響する可能性があります。また、9.9(1) にダウン グレードする方法もあります。

9.8 ガイドライン

- 9.8(2) 以降にアップグレードする前に、FIPS モードではフェールオーバーキーを 14 文字以上にする必要があります。FIPS モードで 9.8(2) 以降にアップグレードする前に、**failover key** または **failover ipsec pre-shared-key** を 14 文字以上に変更する必要があります。フェールオーバーキーが短すぎる場合、最初のユニットをアップグレードしたときにフェールオーバーキーが拒否され、フェールオーバーキーを有効な値に設定するまで、両方のユニットがアクティブになります。
- Amazon Web サービスの ASAv については 9.8(1) にアップグレードしないようにしてください。CSCve56153 のため、9.8(1) にアップグレードするべきではありません。アップグレード後に、ASAv はアクセス不能になります。代わりに 9.8(1.5) 以降にアップグレードしてください。

9.7 ガイドライン

- VTI および VXLAN VNI 用の 9.7(1) ～ 9.7(1.X) およびそれ以降のアップグレードに関する問題：Virtual Tunnel Interfaces（VTI）と VXLAN Virtual Network Identifier（VNI）の両方のインターフェイスを設定すると、フェールオーバー用のゼロ ダウンタイム アップグレードは実行できません。両方のユニットが同じバージョンになるまでは、これらのインターフェイス タイプの接続はスタンバイ ユニットに複製されません。（CSCvc83062）

9.6 ガイドライン

- （ASA 9.6(2) ～ 9.7(x)）SSH 公開キー認証使用時のアップグレードの影響：SSH 認証が更新されることにより、SSH 公開キー認証を有効にするための新たな設定が必要となります。そのため、公開キー認証を使用した既存の SSH 設定はアップグレード後機能しません。公開キー認証は、Amazon Web サービス（AWS）の ASAv のデフォルトであるため、AWS のユーザはこの問題を確認する必要があります。SSH 接続を失う問題を避けるには、アップグレードの前に設定を更新します。または（ASDM アクセスが有効になっている場合）アップグレード後に ASDM を使用して設定を修正できます。

  （注） 元の行動が 9.8(1) で復元されました。

  ユーザ名が「admin」の場合の設定例を示します。

```
username admin nopassword privilege 15
username admin attributes
  ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
  07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
```

  ssh authentication コマンドを使用するには、アップグレードの前に次のコマンドを入力します。

```
aaa authentication ssh console LOCAL
```

```
username admin password <password> privilege 15
```

nopassword キーワードが存在している場合、これを維持するのではなく、代わりにユーザ名に対応したパスワードを設定することを推奨します。**nopassword** キーワードは、パスワードの入力不可を意味するのではなく、任意のパスワードを入力できます。9.6(2) より前のバージョンでは、**aaa** コマンドは SSH 公開キー認証に必須ではありませんでした。このため、**nopassword** キーワードはトリガーされませんでした。本バージョンより **aaa** コマンドは必須となり、**password**（または **nopassword**）キーワードが存在する場合、自動的に **username** の通常のパスワード認証を許可するようになりました。

アップグレード後は、**username** コマンドに対する **password** または **nopassword** キーワードの指定は任意となり、ユーザがパスワードを入力できないように指定できます。よって、公開キー認証のみを強制的に使用する場合は、**username** コマンドを入力しなおします。

```
username admin privilege 15
```

- Firepower 9300 で ASA をアップグレードする場合のアップグレードの影響：バックエンドにおけるライセンス権限付与名義の変更により、ASA 9.6(1)/FXOS 1.1(4) にアップグレードした場合、最初のリロードの際にスタートアップ コンフィギュレーションが正しく解析されず、アドオンの権利付与に対応する設定が拒否されることがあります。

  スタンドアロン ASA では、新バージョンでのリロード後、権限付与が処理され、「承認済み」状態になるのを待ち（[show license all] または [Monitoring] > [Properties] > [Smart License]）、そのまま設定を保存しないで、もう一度リロード（[reload] または [Tools] > [System Reload]）してください。リロードすると、スタートアップ コンフィギュレーションが正しく解析されます。

  フェールオーバーペアにアドオンの権限付与がある場合は、FXOS リリースノートのアップグレード手順に従い、さらに各装置のリロード後にフェールオーバーをリセットしてください（**failover reset** または **[Monitoring] > [Properties] > [Failover] > [Status]**、**[Monitoring] > [Failover] > [System]** または **[Monitoring] > [Failover] > [Failover Group]** を選択後、**Reset Failover** をクリック）。

  クラスタに関しては、FXOS のリリース ノートのアップグレード手順に従います。以降、さらなる操作は不要です。

9.5 のガイドラインおよび移行

- 9.5(2) 新しいキャリア ライセンス：新しいキャリア ライセンスは既存の GTP/GPRS ライセンスを置き換え、SCTP と Diameter インスペクションもサポートします。Firepower 9300 ASA セキュリティ モジュールの場合、**feature mobile-sp** コマンドは **feature carrier** コマンドに自動的に移行します。
- 廃止された 9.5(2) 電子メール プロキシ コマンド：ASA バージョン 9.5(2) では、電子メール プロキシ コマンド（**imap4s**、**pop3s**、**smtps**）およびサブコマンドはサポートされなくなりました。

- 廃止または移行された 9.5(2) CSD コマンド：ASA バージョン 9.5(2) では、CSD コマンド（**csd image**、**show webvpn csd image**、**show webvpn csd**、**show webvpn csd hostscan**、**show webvpn csd hostscan image**）はサポートされなくなりました。

  次の CSD コマンドは移行されます：**csd enable** は **hostscan enable** に移行、**csd hostscan image** は **hostscan image** に移行。

- 廃止された 9.5(2) Select AAA コマンド：ASA バージョン 9.5(2) では、次の AAA コマンドおよびサブコマンド（**override-account-disable**、**authentication crack**）はサポートされなくなりました。

- 9.5(1) 次のコマンドが廃止されました。 **timeout gsn**

- ASA 5508-X および 5516-X を 9.5（x）以降へアップグレードする場合における問題：ASA バージョン 9.5（x）以降へアップグレードする前に、ジャンボフレーム予約を一度も有効にしたことがない場合は、最大のメモリフットプリントをチェックする必要があります。製造上の不具合により、ソフトウェアのメモリ制限が誤って適用されていることがあります。以下の修正を適用せずに 9.5（x）以降にアップグレードした場合、デバイスはブートアップ時にクラッシュします。この場合、ROMMON （「Load an Image for the ASA 5500-X Series Using ROMMON」） を使用して 9.4 にダウングレードし、次の手順を実行して再度アップグレードする必要があります。

  1. 次のコマンドを入力して障害のステータスをチェックします。

     ```
     ciscoasa# show memory detail | include Max memory footprint
     Max memory footprint        =    456384512
     Max memory footprint        =            0
     Max memory footprint        =    456384512
     ```

     456,384,512 より少ない値が [Max memory footprint] に戻される場合は障害が発生しているため、アップグレード前に次の手順を実施する必要があります。表示されるメモリが 456,384,512 以上であれば、この手順の残りをスキップして通常通りにアップグレードできます。

  2. グローバル コンフィギュレーション モードを開始します。

     ```
     ciscoasa# configure terminal
     ciscoasa(config)#
     ```

  3. 一時的にジャンボフレーム予約を有効にします。

     ```
     ciscoasa(config)# jumbo-frame reservation
     WARNING: This command will take effect after the running-config
     is saved and the system has been rebooted. Command accepted.
     INFO: Interface MTU should be increased to avoid fragmenting
     jumbo frames during transmit
     ```

     （注） ASA はリロードしません。

4. 設定を保存します。

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

5. ジャンボフレーム予約を無効にします。

```
ciscoasa(config)# no jumbo-frame reservation
WARNING: This command will take effect after the running-config is saved and
the system has been rebooted. Command accepted.
```

（注） ASA はリロードしません。

6. コンフィギュレーション ファイルを再保存します。

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

7. これで、バージョン 9.5（x）以降へアップグレードできます。

9.4 のガイドラインおよび移行

- 9.4(1) ユニファイド コミュニケーション電話プロキシと Intercompany Media Engine プロキシは非推奨：ASA バージョン 9.4 では、電話プロキシと IME プロキシはサポートされません。

9.3 のガイドラインおよび移行

- 9.3(2) Transport Layer Security（TLS）バージョン 1.2 のサポート：ASDM、クライアントレス SSVPN、および AnyConnect VPN のセキュアなメッセージ送信を実現するため、TLS バージョン 1.2 をサポートします。次のコマンドが導入または変更されました。ssl client-version、ssl server-version、ssl cipher、ssl trust-point、ssl dh-group。次のコマンドが非推奨になりました。ssl encryption
- 9.3(1) AAA Windows NT ドメイン認証の廃止：リモート アクセス VPN ユーザの NTLM サポートを廃止しました。次のコマンドが非推奨になりました。aaa-server protocol nt

9.2 のガイドラインおよび移行

Auto Update Server 証明書の確認

9.2(1) デフォルトでイネーブルになる Auto Update Server 証明書の確認。Auto Update Server 証明書の確認がデフォルトでイネーブルになりました。新しい設定では、証明書の確認を明示的にディセーブルにする必要があります。証明書の確認をイネーブルにしていなかった場合に、以前のリリースからアップグレードしようとすると、証明書の確認はイネーブルではなく、次の警告が表示されます。

```
WARNING: The certificate provided by the auto-update servers will not be verified. In
order to verify this certificate please use the verify-certificate option.
```

設定を移行する場合は、次のように確認なしを明示的に設定します。

auto-update server no-verification

ASDM ログインへのアップグレードの影響

リリース 9.2(2.4) より前のバージョンから 9.2(2.4) 以降にアップグレードした場合の ASDM ログインへのアップグレードの影響。リリース 9.2(2.4) より前のバージョンから ASA バージョン 9.2(2.4) 以降にアップグレードし、コマンド認可と ASDM 定義のユーザ ロールを使用している場合、読み取り専用アクセス権限をもつユーザは ASDM にログインできなくなります。アップグレードの前または後に、**more** コマンドを特権レベル 5 に変更する必要があります。この変更は管理者ユーザのみができます。ASDM バージョン 7.3(2) 以降には定義済みユーザ ロールにレベル 5 の **more** コマンドが含まれますが、既存の設定を手作業で修正する必要があります。

ASDM：

1. [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization] の順に選択し、[Configure Command Privileges] をクリックします。
2. [more] を選択し、[Edit] をクリックします。

3. [Privilege Level] を 5 に変更し、[OK] をクリックします。
4. [OK]、続いて [Apply] をクリックします。

CLI：

```
ciscoasa(config)# privilege cmd level 5 mode exec command more
```

9.1 のガイドラインおよび移行

- 現在の最大 MTU は 9198 バイト：MTU が 9198 を超える値に設定されている場合は、アップグレード時に MTU が自動的に削減されます。場合によっては、この MTU の変更により MTU の不一致が発生する可能性があります。接続している機器が新しい MTU 値を使用するように設定されていることを確認してください。ASA で使用できる最大の MTU は

9198 バイトです（CLI のヘルプでご使用のモデルの正確な最大値を確認してください）。この値にはレイヤ 2 ヘッダーは含まれません。以前は、ASA で 65535 バイトの最大 MTU を指定できましたが、これは不正確であり、問題が発生する可能性がありました。

9.0 のガイドラインおよび移行

- **IPv6 ACL の移行**：IPv6 ACL（**ipv6 access-list**）は、拡張 ACL に移行されます（**access-list extended**）。IPv6 ACL はサポートされなくなりました。

  IPv4 ACL と IPv6 ACL がインターフェイス（**access-group** コマンド）の同じ方向に適用される場合、ACL がマージされます。

  - IPv4 ACL と IPv6 ACL のいずれも access-group 以外で使用されていない場合、IPv4 ACL の名前がマージ後の ACL に使用されます。IPv6 access-list は削除されます。
  - 少なくとも 1 つの ACL が別の機能で使用されている場合、新しい ACL は *IPv4-ACL-name_IPv6-ACL-name* の名前で作成されます。使用中の ACL は、その他の機能に引き続き使用されます。使用されていない ACL は削除されます。IPv6 ACL が別の機能に使用されている場合は、同じ名前の拡張 ACL に移行されます。

- **ACL Any Keyword の移行**：ACL では IPv4 と IPv6 の両方がサポートされるようになり、**any** キーワードが「すべての IPv4 トラフィックと IPv6 トラフィック」を表すようになりました。**any** キーワードを使用するすべての既存の ACL は、「すべての IPv4 トラフィック」を表す **any4** キーワードを使用するように変更されます。

  また、「すべての IPv6 トラフィック」を表す別個のキーワード、**any6** が導入されました。

  any4 および **any6** キーワードは、**any** キーワードを使用するすべてのコマンドで使用できるわけではありません。たとえば、NAT 機能では **any** キーワードのみを使用します。any は、特定の NAT コマンド内のコンテキストに応じて、IPv4 トラフィックまたは IPv6 トラフィックを表します。

- **スタティック NAT とポート変換のアップグレード前の要件**：バージョン 9.0 以降、スタティック NAT とポート変換のルールによって宛先 IP アドレスへのアクセスが制限されるのは、指定されたポートのみです。NAT ルール対象外の別のポートで宛先 IP アドレスにアクセスしようとすると、接続がブロックされます。この動作は Twice NAT の場合も同じです。さらに、Twice NAT ルールの送信元 IP アドレスと一致しないトラフィックが宛先 IP アドレスと一致する場合、宛先ポートに関係なくドロップされます。したがって、宛先 IP アドレスに対して許可される他のすべてのトラフィックのルールをアップグレード前に追加する必要があります。

  たとえば、内部サーバへの HTTP トラフィックをポート 80 とポート 8080 間で変換する次のオブジェクト NAT ルールがあるとします。

```
object network my-http-server
  host 10.10.10.1
  nat (inside,outside) static 192.168.1.1 80 8080
```

  このサーバに FTP などの他のサービスからアクセスする必要がある場合、明示的に許可する必要があります。

```
object network my-ftp-server
  host 10.10.10.1
  nat (inside,outside) static 192.168.1.1 ftp ftp
```

また、サーバの他の複数のポートでトラフィックを許可するために、他のすべてのポートと一致する一般的なスタティック NAT ルールを追加することができます。

```
object network my-server-1
  host 10.10.10.1
  nat (inside,outside) static 192.168.1.1
```

Twice NAT の場合は、192.168.1.0/24 から内部サーバへの HTTP トラフィックを許可し、ポート 80 とポート 8080 間で変換する次のルールがあるとします。

```
object network my-real-server
  host 10.10.10.1
object network my-mapped-server
  host 192.168.1.1
object network outside-real-hosts
  subnet 192.168.1.0 255.255.255.0
object network outside-mapped-hosts
  subnet 10.10.11.0 255.255.255.0
object service http-real
  service tcp destination eq 80
object service http-mapped
  service tcp destination eq 8080
object service ftp-real
  service tcp destination eq 21
nat (outside,inside) source static outside-real-hosts outside-mapped-hosts destination
 static my-mapped-server my-real-server service http-mapped http-real
```

外部のホストから内部サーバの別のサービス（FTP など）にアクセスする必要がある場合は、そのサービスに対して別の NAT ルールを追加します。

```
nat (outside,inside) source static outside-real-hosts outside-mapped-hosts destination
 static my-mapped-server my-real-server ftp-real ftp-real
```

他の発信元アドレスから内部サーバの任意のポートへアクセスする必要がある場合は、その特定の IP アドレスまたは任意の送信元 IP アドレスに対する別の NAT ルールを追加できます。一般的なルールは、特定のルールの後に並べてください。

```
nat (outside,inside) source static any any destination static my-mapped-server
my-real-server
```

8.4 のガイドラインおよび移行

- トランスペアレント モードの設定の移行：8.4 では、すべてのトランスペアレント モードのインターフェイスがブリッジ グループに属します。8.4 にアップグレードすると、既存の 2 つのインターフェイスがブリッジ グループ 1 に配置され、管理 IP アドレスがブリッジ グループ仮想インターフェイス（BVI）に割り当てられます。機能は、1 つのブリッジ

グループを使用する場合と同じです。ブリッジグループ機能を活用して、ブリッジグループごとに最大4つのインターフェイスを設定できます。またシングルモードで、またはコンテキストごとに最大 8 つのブリッジ グループを作成できます。

（注） 8.3 およびそれ以前のバージョンでは、サポートされていない設定として、IPアドレスを使用せずに管理インターフェイスを設定できるほか、デバイス管理アドレスを使用してインターフェイスにアクセスできます。8.4 では、デバイス管理アドレスは BVI に割り当てられるため、その IP アドレスを使用して管理インターフェイスにアクセスできなくなります。管理インターフェイスには独自の IP アドレスが必要です。

- 8.3(1)、8.3(2)、8.4(1) から 8.4(2) にアップグレードする場合、既存の機能を保持するため、すべてのアイデンティティ NAT コンフィギュレーションに **no-proxy-arp** キーワードと **route-lookup** キーワードが含まれるようになりました。**unidirectional** キーワードが削除されました。

8.3 のガイドラインおよび移行

次のマニュアルでは、Cisco ASA 5500 オペレーティング システム（OS）を 8.3 より前のバージョンからバージョン 8.3 にアップグレードする場合の設定の移行プロセスについて説明します。

Cisco ASA 5500 Migration to Version 8.3

クラスタリングのガイドライン

次の例外を除いて、ASA クラスタリングのゼロ ダウンタイム アップグレードに関する特別な要件はありません。

（注） ゼロ ダウンタイム ダウングレードは、正式にはクラスタリングでサポートされていません。

- Firepower 4100/9300 フェールオーバーとフローオフロードのクラスタリング ヒットレス アップグレードの要件：フローオフロード機能でのバグ修正により、FXOS と ASA のいくつかの組み合わせはフローオフロードをサポートしていません（Firepower 4100/9300 と ASA または FTD の互換性を参照）。フローオフロードは、ASA のデフォルトでは無効になっています。フローオフロードの使用時にフェールオーバーまたはクラスタリング ヒットレス アップグレードを実行するには、次のアップグレードパスに従って、FXOS 2.3.1.130 以降にアップグレードする際に常に互換性のある組み合わせを実行していることを確認する必要があります。

  1. ASA を 9.8(3) 以降にアップグレードします。
  2. FXOS を 2.3.1.130 以降にアップグレードします。

3. ASA を最終バージョンにアップグレードします。

たとえば、FXOS 2.2.2.26/ASA 9.8(1) を実行していて、FXOS 2.6.1/ASA 9.12(1) にアップグレードする場合は、次を実行できます。

1. ASA を 9.8(4) にアップグレードします。
2. FXOS を 2.6.1 アップグレードします。
3. ASA を 9.12(1) にアップグレードします。

- Firepower 4100/9300 クラスタを FXOS 2.3/ASA 9.9(2) にアップグレード：制御ユニットが FXOS 2.3/9.9(2) 以降で動作している場合、9.8 以前の ASA 上のデータユニットはクラスタに再参加できません。それらのデータユニットは、ASA バージョンを 9.9(2)+ にアップグレードした後に参加できます [CSCvi54844]。
- 分散サイト間 VPN：障害の発生したユニットでの分散サイト間 VPN セッションは他のユニットで安定するまでに最大 30 分かかります。この間は、さらなるユニット障害によってセッションが失われる可能性があります。このため、クラスタのアップグレード時は、トラフィックの損失を防ぐために次の手順を実行してください。これらの手順をアップグレード タスクに統合するには、FXOS/ASA クラスタのアップグレード手順を参照してください。

（注） 9.9(1) から 9.9(2) 以降にアップグレードする場合、ゼロ ダウンタイム アップグレードは分散サイト間 VPN ではサポートされません。9.9(2) でのアクティブ セッション再配布の機能拡張のために、一部のユニットを 9.9(2) で実行し他のユニットを 9.9(1) で実行することはできません。

1. 制御ユニットのないシャーシでは、ASA コンソールを使用して 1 つのモジュールでクラスタリングを無効にします。

   cluster group *name*

   no enable

   このシャーシ上の FXOS と ASA をアップグレードする場合は、シャーシの再起動後にクラスタリングが無効になるように設定を保存します。

   write memory

2. クラスタが安定するのを待ちます。すべてのバックアップセッションが作成されたことを確認してください。

   show cluster vpn-sessiondb summary

3. このシャーシ上のモジュールごとに、手順 1 と 2 を繰り返します。
4. FXOS CLI または Firepower Chassis Manager を使用してシャーシ上の FXOS をアップグレードします。

5. シャーシがオンラインになったら、FXOS CLI または Firepower Chassis Manager を使用して各モジュール上の ASA イメージを更新します。
6. モジュールがオンラインになったら、ASA コンソールで各モジュール上のクラスタリングを再度有効にします。

   cluster group *name*

   enable

   write memory
7. 2 番目のシャーシで手順 1 ～ 6 を繰り返します。必ず、まずデータユニットでクラスタリングを無効にしてから、最後に制御ユニットでクラスタリングを無効にしてください。

   新しい制御ユニットが、アップグレードされたシャーシから選択されます。
8. クラスタが安定したら、制御ユニットで ASA コンソールを使用して、クラスタ内のすべてのモジュール間でアクティブ セッションを再配布します。

   cluster redistribute vpn-sessiondb

- クラスタリングを含む 9.9(1) 以降に関するアップグレードの問題：9.9(1) 以降では、バックアップの配布が改善されています。新しいバックアップ配布方法を利用するには、次の手順で 9.9(1) 以降へのアップグレードを実行する必要があります。これを行わない場合、アップグレードされたユニットは引き続き古い方法を使用します。
  1. クラスタからすべてのセカンダリ ユニットを削除します（クラスタはプライマリ ユニットのみで構成されます）。
  2. 1 つのセカンダリ ユニットをアップグレードし、クラスタに再参加させます。
  3. プライマリ ユニットでクラスタリングを無効にします。そのユニットをアップグレードし、クラスタに再参加させます。
  4. 残りのセカンダリ ユニットをアップグレードし、それらを一度に 1 つずつクラスタに再参加させます。

- Firepower 4100/9300 クラスタの ASA 9.8(1) 以前へのアップグレード：アップグレードプロセスの一部であるデータユニット（**no enable**）のクラスタリングを無効にすると、そのユニット宛てのトラフィックは、トラフィックが新しい所有者 [CSCvc85008] にリダイレクトされるまで、最大で 3 秒間ドロップされる場合があります。
- CSCvb24585 に関する修正が行われている次のリリースにアップグレードする場合は、ゼロ ダウンタイム アップグレードがサポートされない可能性があります。この修正により、3DES がデフォルト（中レベル）の SSL 暗号から低レベルの暗号セットに移行されました。3DES のみを含むカスタム暗号を設定する場合、接続の相手側が 3DES を含まないデフォルト（中レベル）の暗号を使用していると、不一致が生じる可能性があります。
  - 9.1(7.12)
  - 9.2(4.18)

- 9.4(3.12)
- 9.4(4)
- 9.5(3.2)
- 9.6(2.4)
- 9.6(3)
- 9.7(1)
- 9.8(1)

- 完全修飾ドメイン名（FQDN）ACL のアップグレードに関する問題：CSCuv92371 が原因で、FQDN を含む ACL は、クラスタまたはフェールオーバー ペアのセカンダリ ユニットへの不完全な ACL 複製を引き起こす可能性があります。このバグは、9.1(7)、9.5(2)、9.6(1)、およびいくつかの暫定リリースにおいて発生します。CSCuy34265 の修正プログラムを含む 9.1(7.6) 以降、9.5(3) 以降、9.6(2) 以降にアップグレードすることをお勧めします。ただし、設定の複製の性質上、ゼロ ダウンタイム アップグレードは使用できません。さまざまなアップグレード方法の詳細については、CSCuy34265 を参照してください。

- Firepower Threat Defense バージョン 6.1.0 クラスタは、サイト間クラスタリングをサポートしていません（6.2.0 以降では FlexConfig を使用してサイト間機能を設定できます）。FXOS 2.1.1 で 6.1.0 クラスタを展開または再展開している場合、（サポートされていない）サイト ID の値を入力しているときは、6.2.3 にアップグレードする前に、FXOS の各ユニットでサイト ID を削除（**0** に設定）する必要があります。これを行わない場合、ユニットはアップグレード後にクラスタに再参加できません。すでにアップグレード済みの場合は、各ユニットでサイト ID を **0** に変更して問題を解決してください。サイト ID を表示または変更するには、FXOS の構成ガイドを参照してください。

- 9.5(2) 以降へのアップグレード（CSCuv82933）：制御ユニットをアップグレードする前に「**show cluster info**」と入力すると、アップグレードされたデータユニットが「DEPUTY_BULK_SYNC」と表示されます。他にも正しい状態と一致しない状態が表示されます。すべてのユニットをアップグレードすると状態が正しく表示されるようになるので、この表示は無視しても構いません。

- 9.0(1) または 9.1(1) からのアップグレード（CSCue72961）：ゼロ ダウンタイム アップグレードはサポートされていません。

フェールオーバーのガイドライン

次の例外を除き、フェールオーバー用のゼロ ダウンタイム アップグレードに関する特別な要件はありません。

- Firepower 1010 では、無効な VLAN ID によって問題が発生する可能性があります。9.15(1) にアップグレードする前に、3968 ー 4047 の範囲内のスイッチポートに VLAN を使用していないことを確認してください。これらの ID は内部使用専用であり、9.15(1) には、これらの ID を使用していないことを確認するチェックが含まれます。たとえば、フェールオー

バーペアのアップグレード後にこれらの ID が使用されていた場合、フェールオーバーペアは一時停止状態になります。詳細については、「CSCvw33057」を参照してください。

- Firepower 4100/9300 フェールオーバーとフローオフロードのクラスタリング ヒットレス アップグレードの要件：フローオフロード機能でのバグ修正により、FXOS と ASA のいくつかの組み合わせはフローオフロードをサポートしていません（Firepower 4100/9300 と ASA または FTD の互換性を参照）。フローオフロードは、ASA のデフォルトでは無効になっています。フローオフロードの使用時にフェールオーバーまたはクラスタリング ヒットレス アップグレードを実行するには、次のアップグレードパスに従って、FXOS 2.3.1.130 以降にアップグレードする際に常に互換性のある組み合わせを実行していることを確認する必要があります。

  1. ASA を 9.8(3) 以降にアップグレードします。
  2. FXOS を 2.3.1.130 以降にアップグレードします。
  3. ASA を最終バージョンにアップグレードします。

  たとえば、FXOS 2.2.2.26/ASA 9.8(1) を実行していて、FXOS 2.6.1/ASA 9.12(1) にアップグレードする場合は、次を実行できます。

  1. ASA を 9.8(4) にアップグレードします。
  2. FXOS を 2.6.1 アップグレードします。
  3. ASA を 9.12(1) にアップグレードします。

- 8.4(6)、9.0(2)、および 9.1(2) のアップグレードの問題：CSCug88962 が原因で、8.4(6)、9.0(2)、および 9.1(3) へのゼロ ダウンタイム アップグレードを実行することはできません。代わりに 8.4(5) または 9.0(3) にアップグレードする必要があります。9.1(1) をアップグレードする場合、CSCuh25271 が原因で、9.1(3) リリースに直接アップグレードすることはできません。したがってゼロ ダウンタイム アップグレードのための回避策はありません。9.1 (3) 以降にアップグレードする前に、9.1(2) にアップグレードする必要があります。

- 完全修飾ドメイン名（FQDN）ACL のアップグレードに関する問題：CSCuv92371 が原因で、FQDN を含む ACL は、クラスタまたはフェールオーバー ペアのセカンダリ ユニットへの不完全な ACL 複製を引き起こす可能性があります。このバグは、9.1(7)、9.5(2)、9.6(1)、およびいくつかの暫定リリースにおいて発生します。CSCuy34265 の修正プログラムを含む 9.1(7.6) 以降、9.5(3) 以降、9.6(2) 以降にアップグレードすることをお勧めします。ただし、設定の複製の性質上、ゼロ ダウンタイム アップグレードは使用できません。さまざまなアップグレード方法の詳細については、CSCuy34265 を参照してください。

- VTI および VXLAN VNI 用の 9.7(1) ～ 9.7(1.X) およびそれ以降のアップグレードに関する問題：Virtual Tunnel Interfaces（VTI）と VXLAN Virtual Network Identifier（VNI）の両方のインターフェイスを設定すると、フェールオーバー用のゼロ ダウンタイム アップグレードは実行できません。両方のユニットが同じバージョンになるまでは、これらのインターフェイス タイプの接続はスタンバイ ユニットに複製されません。（CSCvc83062）

- 9.8(2) 以降にアップグレードする前に、FIPS モードではフェールオーバーキーを 14 文字以上にする必要があります。FIPS モードで 9.8(2) 以降にアップグレードする前に、**failover key** または **failover ipsec pre-shared-key** を 14 文字以上に変更する必要があります。フェールオーバーキーが短すぎる場合、最初のユニットをアップグレードしたときにフェールオーバーキーが拒否され、フェールオーバーキーを有効な値に設定するまで、両方のユニットがアクティブになります。
- GTP インスペクションのアップグレードの問題：GTP のデータ構造が新しいノードに複製されないため、アップグレード中にダウンタイムが発生する可能性があります。

その他のガイドライン

- Cisco ASA クライアントレス SSL VPN ポータルのカスタマイズにおける整合性の脆弱性：ASA 上のクライアントレス SSL VPN に対して複数の脆弱性修正が行われているため、修正版へソフトウェアをアップグレードする必要があります。脆弱性と ASA の修正済みバージョンについて、http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141008-asa を参照してください。脆弱性をもった構成で以前のバージョンの ASA を運用したことがある場合は、現在実行中のバージョンに関係なく、ポータルのカスタマイズが危殆化されていないか確認する必要があります。過去に攻撃者がカスタマイゼーション オブジェクトを危殆化した場合、ASA を修正版にアップグレードした後にも危殆化されたオブジェクトが存続します。ASA をアップグレードすることで今後の危殆化を阻止できますが、すでに危殆化されているカスタマイゼーション オブジェクトは一切変更されず、システムに存続します。

Firepower Management Center のアップ グレード ガイドライン

アップグレードを行う前に、『FMC Upgrade Guide』の Firepower Management Center に関するガイドラインを確認してください。

FXOS のアップグレード ガイドライン

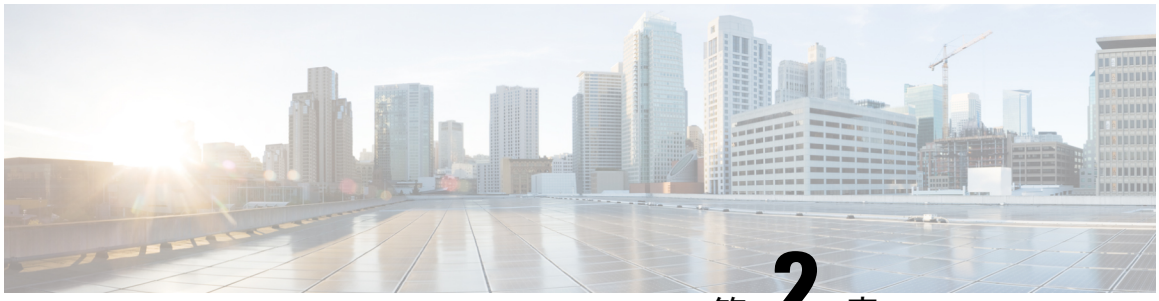
アップグレードする前に、選択したアップグレードパスの各 FXOS バージョンのリリース ノートをお読みください。リリース ノートには、新機能や変更された機能を含む、各 FXOS リリースに関する重要な情報が記載されています。

アップグレードを行うには、対処する必要のある設定変更が必要な場合があります。たとえば、FXOS リリースでサポートされている新しいハードウェアが、FXOS ファームウェアの更新を要求する場合があります。

FXOS リリース ノートはこちらから入手できます：https://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html。

構成のバックアップ

アップグレードの前に構成およびその他の重要なファイルをバックアップすることをお勧めします（特に設定を移行する場合）。オペレーティングシステムごとにバックアップの方法が異なります。詳細については、ASA、ASDM、ASA FirePower ローカル管理、Firepower Management Center、および FXOS 設定の各ガイドを参照してください。



第 2 章

ASA アプライアンスまたは ASAv のアップグレード

このドキュメントに記載されている手順により、ASA 5500-X、FirePOWER 2100 のASA、ASAv、ASASM、および ISA 3000 をアップグレードできます。

- Firepower 1000 または Firepower 2100 のアップグレード （85 ページ）
- ASA 5500-X、ASAv、ASASM、ISA 3000 のアップグレード （118 ページ）

Firepower 1000 または Firepower 2100 のアップグレード

このドキュメントでは、Firepower 1000 および 2100 シリーズのスタンドアロンまたはフェールオーバー展開用に、ASA、FXOS、および ASDM のアップグレードを計画し、実装する方法について説明します。

Firepower 2100 9.12 以前では、プラットフォームモードのみを使用できます。9.13 以降では、アプライアンスモードがデフォルトです。モードを確認するには、ASA CLI で **show fxos mode** コマンドを使用します。Firepower 1000 はアプライアンスモードでのみ実行されます。

アプライアンスモードでの Firepower 1000 および Firepower 2100 のアップグレード

このドキュメントでは、アプライアンスモードの Firepower 1000 および 2100 のスタンドアロンまたはフェールオーバー展開用に、ASA、FXOS、および ASDM のアップグレードを計画し、実装する方法について説明します。バージョン 9.13 以前では、Firepower 2100 はプラットフォームモードのみをサポートしていました。9.14 以降では、アプライアンスモードがデフォルトです。9.14 以降では、ASA で **show fxos mode** コマンドを使用して現在のモードを決定します。プラットフォームモードの手順については、プラットフォームモードでの Firepower 2100 のアップグレード （100 ページ） を参照してください。

スタンドアロン ユニットのアップグレード

スタンドアロン ユニットをアップグレードするには CLI または ASDM を使用します。

CLI を使用したスタンドアロン ユニットのアップグレード

このセクションでは、アプライアンスモードの Firepower 1000 または 2100 に ASDM および ASA イメージをインストールする方法について説明します。

始める前に

この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバタイプについては、『ASA Command Reference』の **copy** コマンドを参照してください。

手順

ステップ 1 特権 EXEC モードで、ASA ソフトウェアをフラッシュメモリにコピーします。

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

例：

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA
disk0:/cisco-asa-fp1k.9.14.1.SPA
```

ステップ 2 ASDM イメージをフラッシュメモリにコピーします。

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

例：

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-7141.bin disk0:/asdm-7141.bin
```

ステップ 3 グローバル コンフィギュレーション モードにアクセスします。

configure terminal

例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

ステップ 4 設定されている現在のブートイメージが存在している場合、これを表示します。

show running-config boot system

設定に **boot system** コマンドが存在しない場合があることに注意してください。たとえば、ROMMON からイメージをインストールした場合、新しいデバイスがある場合、またはコマンドを手動で削除した場合などです。

例：

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

ステップ 5 **boot system** コマンドが設定されている場合は、新しいブートイメージを入力できるようにコマンドを削除します。

no boot system disk*n*:/[*path*/]*asa_image_name*

boot system コマンドが設定されていない場合は、この手順をスキップします。

例：

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

ステップ 6 ブートする ASA イメージを設定します（先ほどアップロードしたもの）。

boot system disk*n*:/[*path*/]*asa_image_name*

boot system コマンドは 1 つだけ入力できます。**boot system** コマンドは、入力時にアクションを実行します。システムはイメージを検証して解凍し、ブート場所（FXOS によって管理される disk0 の内部ロケーション）にコピーします。ASA をリロードすると、新しいイメージがロードされます。リロードの前に気が変わった場合は、**no boot system** コマンドを入力してブート場所から新しいイメージを削除し、現在のイメージを引き続き実行することができます。

例：

```
ciscoasa(config)# boot system disk0:/cisco-asa-fp1k.9.14.1.SPA

The system is currently installed with security software package 9.13.1, which has:
   - The platform version:  2.7.1
   - The CSP (asa) version: 9.13.1
Preparing new image for install...
!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.14.1 will do the following:
   - upgrade to the new platform version 2.8.1
   - upgrade to the CSP ASA version 9.14.1
After the installation is complete, reload to apply the new image.
Finalizing image install process...

Install_status: ready...........
Install_status: validating-images.....
Install_status: update-software-pack-completed
ciscoasa(config)#
```

ステップ 7 使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

asdm image disk*n*:/[*path*/]*asdm_image_name*

使用するように設定できる ASDM イメージは 1 つだけです。この場合、最初に既存のコンフィギュレーションを削除する必要はありません。

例：

```
ciscoasa(config)# asdm image disk0:/asdm-7141.bin
```

ステップ 8 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

ステップ 9 ASA をリロードします。

reload

ASDM を使用したローカルコンピュータからのスタンドアロンユニットのアップグレード

Upgrade Software from Local Computer ツールにより、コンピュータからフラッシュファイルシステムにイメージファイルをアップロードし、アプライアンスモードの Firepower 1000 または 2100 の ASA をアップグレードできます。

手順

ステップ 1 メイン ASDM アプリケーション ウィンドウで、**[Tools]** > **[Upgrade Software from Local Computer]** の順に選択します。

[Upgrade Software] ダイアログボックスが表示されます。

ステップ 2 [Image to Upload] ドロップダウンリストから、[ASDM] を選択します。

ステップ 3 [Local File Path] フィールドで [Browse Local Files] をクリックして PC 上のファイルを見つけます。

ステップ 4 [Flash File System Path] フィールドで [Browse Flash] をクリックしてフラッシュ ファイル システム上のディレクトリまたはファイルを見つけます。

ステップ 5 [Upload Image] をクリックします。

アップグレード プロセスには数分かかる場合があります。

ステップ 6 このイメージを ASDM イメージとして設定するように求められます。[Yes] をクリックします。

ステップ 7 ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。

アップグレード ツールを終了します。**注**：ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM を終了して再接続します。

ステップ 8 これらの手順を繰り返し、[Image to Upload] ドロップダウンリストで [ASA] を選択します。この手順は、その他のタイプのファイルのアップロードでも同じです。

ステップ 9 **[Tools]** > **[System Reload]** を選択して、ASA をリロードします。

リロードの詳細の確認を求める新しいウィンドウが表示されます。

a) [Save the running configuration at the time of reload] オプション ボタン（デフォルト）をクリックします。
b) リロードする時刻を選択します（たとえば、デフォルトの [Now]）。
c) [Schedule Reload] をクリックします。

リロードが開始されると、[Reload Status] ウィンドウにリロードの進行状況が表示されます。ASDM を終了するオプションも表示されます。

ステップ 10 ASA のリロード後、ASDM を再起動します。

コンソールポートでリロードの状況を確認できます。または、数分待った後に ASDM を使用して、接続可能になるまで再試行することもできます。

ASDM Cisco.com ウィザードを使用したスタンドアロンユニットのアップグレード

アプライアンスモードの Firepower 1000 または 2100 の場合、**Upgrade Software from Cisco.com Wizard** により、ASDM および ASA を最新のバージョンに自動的にアップグレードできます。

このウィザードでは、次の操作を実行できます。

- アップグレード用の ASA イメージファイルまたは ASDM イメージファイルを選択する。

（注） ASDM は最新のイメージバージョンをダウンロードし、そこにはビルド番号が含まれています。たとえば、9.9(1) をダウンロードする場合に、ダウンロードが 9.9(1.2) となる可能性があります。この動作は想定されているため、計画したアップグレードを続行できます。

- 実行したアップグレードの変更点を確認する。
- イメージをダウンロードし、インストールする。
- インストールのステータスを確認する。
- インストールが正常に完了した場合は、ASA をリロードして、コンフィギュレーションを保存し、アップグレードを完了する。

始める前に

内部的な変更により、このウィザードでは ASDM 7.10(1) 以降の使用のみがサポートされています。また、イメージの命名が変更されたため、ASA 9.10(1) 以降にアップグレードするには、ASDM 7.12(1) 以降を使用する必要があります。ASDM は ASA の以前のリリースと下位互換性があるため、実行している ASA バージョンを問わず、ASDM をアップグレードすることができます。

手順

ステップ 1 **[ツール（Tools）]** > **[ASA/ASDM更新のチェック（Check for ASA/ASDM Updates）]** を選択します。

マルチコンテキストモードでは、システムからこのメニューにアクセスします。

[Cisco.com Authentication] ダイアログボックスが表示されます。

ステップ 2 Cisco.com のユーザ ID とパスワードを入力して、[Login] をクリックします。

[Cisco.com Upgrade Wizard] が表示されます。

（注） 利用可能なアップグレードがない場合は、ダイアログボックスが表示されます。ウィザードを終了するには、[OK] をクリックします。

ステップ 3 [Next] をクリックして [Select Software] 画面を表示します。

現在の ASA バージョンおよび ASDM バージョンが表示されます。

ステップ 4 ASA バージョンおよび ASDM バージョンをアップグレードするには、次の手順を実行します。

a) [ASA] 領域で、[Upgrade to] チェックボックスをオンにしてから、アップグレードする ASA バージョンをドロップダウン リストから選択します。

b) [ASDM] 領域で、[Upgrade to] チェックボックスをオンにしてから、アップグレードする ASDM バージョンをドロップダウン リストから選択します。

ステップ 5 [Next] をクリックして [Review Changes] 画面を表示します。

ステップ 6 次の項目を確認します。

- ダウンロードした ASA イメージ ファイルや ASDM イメージ ファイルが正しいファイルであること。
- アップロードする ASA イメージ ファイルや ASDM イメージ ファイルが正しいファイルであること。
- 正しい ASA ブート イメージが選択されていること。

ステップ 7 [Next] をクリックして、アップグレード インストールを開始します。

アップグレード インストールの進行状況を示すステータスを表示できます。

[Results] 画面が表示され、アップグレードインストール ステータス（成功または失敗）など、追加の詳細が示されます。

ステップ 8 アップグレード インストールが成功した場合に、アップグレード バージョンを有効にするには、[Save configuration and reload device now] チェックボックスをオンにして、ASA を再起動し、ASDM を再起動します。

ステップ 9 [Finish] をクリックして、ウィザードを終了し、コンフィギュレーションに対して行った変更を保存します。

（注） 次に高いバージョン（存在する場合）にアップグレードするには、ウィザードを再起動する必要があります。

ステップ 10 ASA のリロード後、ASDM を再起動します。

コンソールポートでリロードの状況を確認できます。または、数分待った後に ASDM を使用して、接続可能になるまで再試行することもできます。

アクティブ/スタンバイ フェールオーバー ペアのアップグレード

アクティブ/スタンバイ フェールオーバー ペアをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、CLI または ASDM を使用します。

CLI を使用したアクティブ/スタンバイ フェールオーバー ペアのアップグレード

アプライアンスモードの Firepower 1000 または 2100 のアクティブ/スタンバイ フェールオーバー ペアをアップグレードするには、次の手順を実行します。

始める前に

- アクティブ装置で次の手順を実行します。SSH アクセスの場合、アクティブな IP アドレスに接続します。アクティブ装置は常にこの IP アドレスを保有しています。CLI に接続する場合は、ASA プロンプトを調べてフェールオーバー ステータスを確認します。フェールオーバー ステータスと優先順位（プライマリまたはセカンダリ）を表示するように ASA プロンプトを設定できます。これは、接続しているユニットを特定するのに役立ちます。prompt コマンドを参照してください。代わりに、**show failover** コマンドを入力して、このユニットのステータスと優先順位（プライマリまたはセカンダリ）を表示します。
- この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバタイプについては、『ASA Command Reference』の **copy** コマンドを参照してください。

手順

ステップ 1 特権 EXEC モード時にアクティブ装置で、ASA ソフトウェアをアクティブ装置のフラッシュ メモリにコピーします。

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

例：

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA
disk0:/cisco-asa-fp1k.9.14.1.SPA
```

ステップ 2 ソフトウェアをスタンバイ装置にコピーします。アクティブ装置で指定したのと同じパスを指定してください。

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

例：

```
asa/act# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA disk0:/cisco-asa-fp1k.9.14.1.SPA
```

ステップ 3 ASDM イメージをアクティブ装置のフラッシュ メモリにコピーします。

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

例：

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-7141.bin disk0:/asdm-7141.bin
```

ステップ 4 ASDMイメージをスタンバイ装置にコピーします。アクティブ装置で指定したのと同じパスを指定してください。

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name*
disk*n***:/**[*path/*]*asdm_image_name*

例：

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-7141.bin
 disk0:/asdm-7141.bin.bin
```

ステップ 5 まだグローバル コンフィギュレーション モードを開始していない場合は、グローバル コンフィギュレーション モードを開始します。

configure terminal

ステップ 6 設定されている現在のブートイメージが存在している場合、これを表示します。

show running-config boot system

設定に **boot system** コマンドが存在しない場合があることに注意してください。たとえば、ROMMONからイメージをインストールした場合、新しいデバイスがある場合、またはコマンドを手動で削除した場合などです。

例：

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

ステップ 7 **boot system** コマンドが設定されている場合は、新しいブートイメージを入力できるようにコマンドを削除します。

no boot system disk*n***:/**[*path/*]*asa_image_name*

boot system コマンドが設定されていない場合は、この手順をスキップします。

例：

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

ステップ 8 ブートする ASA イメージを設定します（先ほどアップロードしたもの）。

boot system disk*n***:/**[*path/*]*asa_image_name*

boot system コマンドは 1 つだけ入力できます。**boot system** コマンドは、入力時にアクションを実行します。システムはイメージを検証して解凍し、ブート場所（FXOS によって管理される disk0 の内部ロケーション）にコピーします。ASA をリロードすると、新しいイメージがロードされます。リロードの前に気が変わった場合は、**no boot system** コマンドを入力してブート場所から新しいイメージを削除し、現在のイメージを引き続き実行することができます。

例：

```
ciscoasa(config)# boot system disk0:/cisco-asa-fp1k.9.14.1.SPA

The system is currently installed with security software package 9.13.1, which has:
   - The platform version:  2.7.1
   - The CSP (asa) version: 9.13.1
Preparing new image for install...
!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.14.1 will do the following:
   - upgrade to the new platform version 2.8.1
   - upgrade to the CSP ASA version 9.14.1
After the installation is complete, reload to apply the new image.
Finalizing image install process...

Install_status: ready...........
Install_status: validating-images.....
Install_status: update-software-pack-completed
ciscoasa(config)#
```

ステップ 9 使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

asdm image disk*n***:/**[*path*/]*asdm_image_name*

例：

```
asa/act(config)# asdm image disk0:/asdm-7141.bin
```

使用するように設定できる ASDM イメージは 1 つだけです。この場合、最初に既存のコンフィギュレーションを削除する必要はありません。

ステップ 10 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

これらの設定変更は、スタンバイ ユニットに自動的に保存されます。

ステップ 11 スタンバイ装置をリロードして新しいイメージを起動します。

failover reload-standby

スタンバイ装置のロードが完了するまで待ちます。**show failover** コマンドを使用して、スタンバイ ユニットが Standby Ready 状態かどうかを検証します。

ステップ 12 強制的にアクティブ装置からスタンバイ装置へのフェールオーバーを行います。

no failover active

SSH セッションから切断されている場合は、新しいアクティブ/元のスタンバイ ユニット上に現在あるメイン IP アドレスに再接続します。

ステップ 13 新しいアクティブ装置から、元のアクティブ装置（今の新しいスタンバイ装置）をリロードします。

failover reload-standby

例：

```
asa/act# failover reload-standby
```

（注） 元のアクティブ ユニットのコンソール ポートに接続されている場合は、代わりに **reload** コマンドを入力して、元のアクティブ ユニットをリロードする必要があります。

ASDM を使用したアクティブ/スタンバイ フェールオーバー ペアのアップグレード

アクティブ/スタンバイ フェールオーバー ペアをアップグレードするには、アプライアンス モードの Firepower 1000 または 2100 に対して次の手順を実行します。

始める前に

ローカル管理コンピュータに ASA と ASDM のイメージを配置します。

手順

ステップ 1 スタンバイ IP アドレスに接続して、*standby* ユニット上で ASDM を起動します。

ステップ 2 メイン ASDM アプリケーションウィンドウで、**[Tools]** > **[Upgrade Software from Local Computer]** の順に選択します。

[Upgrade Software] ダイアログボックスが表示されます。

ステップ 3 [Image to Upload] ドロップダウンリストから、[ASDM] を選択します。

ステップ 4 [Local File Path] フィールドにコンピュータ上のファイルへのローカル パスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを見つけます。

ステップ 5 [Flash File System Path] フィールドにフラッシュファイルシステムへのパスを入力するか、[Browse Flash] をクリックしてフラッシュファイルシステム上のディレクトリまたはファイルを検索します。

ステップ 6 [Upload Image] をクリックします。アップグレード プロセスには数分かかる場合があります。

このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。

ステップ 7 これらの手順を繰り返し、[Image to Upload] ドロップダウン リストで [ASA] を選択します。

このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。

ステップ 8 メイン IP アドレスに接続して ASDM をアクティブなユニットに接続し、スタンバイ ユニットで使用したのと同じファイルの場所を使用して、ASDM ソフトウェアをアップロードします。

ステップ 9 このイメージを ASDM イメージとして設定するように求められたら、[Yes] をクリックします。

ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。アップグレード ツールを終了します。**注**：ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM をリロードします。

ステップ 10 スタンバイ ユニットで使用したのと同じファイルの場所を使用して、ASA ソフトウェアをアップロードします。

ステップ 11 このイメージを ASA イメージとして設定するように求められたら、[Yes] をクリックします。

新しいイメージを使用するために、ASA をリロードするよう求められます。[OK] をクリックします。アップグレード ツールを終了します。

ステップ 12 コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。

これらの設定変更は、スタンバイ ユニットに自動的に保存されます。

ステップ 13 **[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** の順に選択し、**[Reload Standby]** をクリックして、スタンバイ装置をリロードします。

[System] ペインを開いたまま、スタンバイ ユニットがリロードされるのを確認します。

ステップ 14 スタンバイユニットがリロードしたら、**[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** の順に選択し、**[Make Standby]** をクリックして、アクティブユニットをスタンバイユニットにフェールオーバーします。

ASDM は新しいアクティブ ユニットに自動的に再接続されます。

ステップ 15 **[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** の順に選択し、**[Reload Standby]** をクリックして、（新しい）スタンバイユニットをリロードします。

アクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー ペアをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、CLI または ASDM を使用します。

CLI を使用したアクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー コンフィギュレーションの 2 つの装置をアップグレードするには、アプライアンスモードの Firepower 1000 または 2100 で次の手順を実行します。

始める前に

- 標準出荷単位で次の手順を実行します。
- これらの手順をシステム実行スペースで実行します。
- この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバタイプについては、『ASA Command Reference』の **copy** コマンドを参照してください。

手順

ステップ 1 特権 EXEC モード時にプライマリ ユニットで、ASA ソフトウェアをフラッシュ メモリにコピーします。

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

例：

```
asa/act/pri# copy ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA
disk0:/cisco-asa-fp1k.9.14.1.SPA
```

ステップ 2 ソフトウェアをセカンダリ装置にコピーします。プライマリ装置で指定したのと同じパスを指定してください。

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

例：

```
asa/act/pri# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA disk0:/cisco-asa-fp1k.9.14.1.SPA
```

ステップ 3 ASDM イメージをプライマリ装置のフラッシュ メモリにコピーします。

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

例：

```
asa/act/pri# ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-7141.bin
disk0:/asdm-7141.bin
```

ステップ 4 ASDMイメージをセカンダリ装置にコピーします。標準出荷単位で指定したのと同じパスを指定してください。

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

例：

```
asa/act/pri# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asdm-7141.bin disk0:/asdm-7141.bin
```

ステップ 5 まだグローバル コンフィギュレーション モードを開始していない場合は、グローバル コンフィギュレーション モードを開始します。

configure terminal

ステップ 6 設定されている現在のブートイメージが存在している場合、これを表示します。

show running-config boot system

設定に **boot system** コマンドが存在しない場合があることに注意してください。たとえば、ROMMON からイメージをインストールした場合、新しいデバイスがある場合、またはコマンドを手動で削除した場合などです。

例：

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

ステップ 7 **boot system** コマンドが設定されている場合は、新しいブートイメージを入力できるようにコマンドを削除します。

no boot system disk*n***:/**[*path*/]*asa_image_name*

boot system コマンドが設定されていない場合は、この手順をスキップします。

例：

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

ステップ 8 ブートする ASA イメージを設定します（先ほどアップロードしたもの）。

boot system disk*n***:/**[*path*/]*asa_image_name*

boot system コマンドは 1 つだけ入力できます。**boot system** コマンドは、入力時にアクションを実行します。システムはイメージを検証して解凍し、ブート場所（FXOS によって管理される disk0 の内部ロケーション）にコピーします。ASA をリロードすると、新しいイメージがロードされます。リロードの前に気が変わった場合は、**no boot system** コマンドを入力してブート場所から新しいイメージを削除し、現在のイメージを引き続き実行することができます。

例：

```
ciscoasa(config)# boot system disk0:/cisco-asa-fp1k.9.14.1.SPA

The system is currently installed with security software package 9.13.1, which has:
   - The platform version:  2.7.1
   - The CSP (asa) version: 9.13.1
Preparing new image for install...
!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.14.1 will do the following:
   - upgrade to the new platform version 2.8.1
   - upgrade to the CSP ASA version 9.14.1
After the installation is complete, reload to apply the new image.
Finalizing image install process...

Install_status: ready...........
Install_status: validating-images.....
Install_status: update-software-pack-completed
ciscoasa(config)#
```

ステップ 9 使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

asdm image disk*n***:/**[*path*/]*asdm_image_name*

例：

```
asa/act/pri(config)# asdm image disk0:/asdm-7141.bin
```

使用するように設定できるASDMイメージは1つだけです。この場合、最初に既存のコンフィギュレーションを削除する必要はありません。

ステップ 10 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

これらの設定変更は、セカンダリ ユニットに自動的に保存されます。

ステップ 11 プライマリ ユニットの両方のフェールオーバー グループをアクティブにします。

failover active group 1

failover active group 2

例：

```
asa/act/pri(config)# failover active group 1
asa/act/pri(config)# failover active group 2
```

ステップ 12 セカンダリ装置をリロードして新しいイメージを起動します。

failover reload-standby

セカンダリ装置のロードが完了するまで待ちます。**show failover** コマンドを使用して、両方のフェールオーバー グループが Standby Ready 状態であることを確認します。

ステップ 13 セカンダリ装置で、両方のフェールオーバー グループを強制的にアクティブにします。

no failover active group 1

no failover active group 2

例：

```
asa/act/pri(config)# no failover active group 1
asa/act/pri(config)# no failover active group 2
asa/stby/pri(config)#
```

SSH セッションから切断されている場合は、セカンダリ ユニット上に現在あるフェールオーバー グループ 1 の IP アドレスに再接続します。

ステップ 14 プライマリ装置をリロードします。

failover reload-standby

例：

```
asa/act/sec# failover reload-standby
```

（注） プライマリ ユニットのコンソール ポートに接続されている場合は、代わりに **reload** コマンドを入力して、プライマリ ユニットをリロードする必要があります。

SSH セッションから切断される場合があります。

ステップ 15 フェールオーバー グループは、**preempt** コマンドを使用して設定されている場合、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。

ASDM を使用したアクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー コンフィギュレーションの 2 つの装置をアップグレードするには、アプライアンスモードの Firepower 1000 または 2100 で次の手順を実行します。

始める前に

- これらの手順をシステム実行スペースで実行します。
- ローカル管理コンピュータに ASA と ASDM のイメージを配置します。

手順

ステップ 1 フェールオーバー グループ 2 の管理アドレスに接続して、セカンダリ ユニットで ASDM を起動します。

ステップ 2 メイン ASDM アプリケーションウィンドウで、**[Tools] > [Upgrade Software from Local Computer]** の順に選択します。

[Upgrade Software] ダイアログボックスが表示されます。

ステップ 3 [Image to Upload] ドロップダウンリストから、[ASDM] を選択します。

ステップ 4 [Local File Path] フィールドにコンピュータ上のファイルへのローカル パスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを見つけます。

ステップ 5 [Flash File System Path] フィールドにフラッシュファイルシステムへのパスを入力するか、[Browse Flash] をクリックしてフラッシュファイルシステム上のディレクトリまたはファイルを検索します。

ステップ 6 [Upload Image] をクリックします。アップグレード プロセスには数分かかる場合があります。

このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。

ステップ 7 これらの手順を繰り返し、[Image to Upload] ドロップダウン リストで [ASA] を選択します。

このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。

ステップ 8 フェールオーバー グループ 1 の管理 IP アドレスに接続して ASDM をプライマリ ユニットに接続し、セカンダリ ユニットで使用したのと同じファイルの場所を使用して、ASDM ソフトウェアをアップロードします。

ステップ 9 このイメージを ASDM イメージとして設定するように求められたら、[Yes] をクリックします。

ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。アップグレード ツールを終了します。**注**：ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM をリロードします。

ステップ 10 セカンダリユニットで使用したのと同じファイルの場所を使用して、ASA ソフトウェアをアップロードします。

ステップ 11 このイメージを ASA イメージとして設定するように求められたら、[Yes] をクリックします。

新しいイメージを使用するために、ASA をリロードするよう求められます。[OK] をクリックします。アップグレード ツールを終了します。

ステップ 12 コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。

これらの設定変更は、セカンダリ ユニットに自動的に保存されます。

ステップ 13 **[Monitoring]** > **[Failover]** > **[Failover Group #]** の順に選択して、プライマリユニット上の両方のフェールオーバーグループをアクティブにします。ここで **#** は、プライマリユニットに移動するフェールオーバーグループの数です。**[Make Active]** をクリックします。

ステップ 14 **[Monitoring]** > **[Failover]** > **[System]** の順に選択し、**[Reload Standby]** をクリックして、セカンダリユニットをリロードします。

[System] ペインを開いたまま、セカンダリ ユニットがリロードされるのを確認します。

ステップ 15 セカンダリユニットが起動したら、**[Monitoring]** > **[Failover]** > **[Failover Group #]** の順に選択して、セカンダリユニット上の両方のフェールオーバーグループをアクティブにします。ここで **#** は、セカンダリユニットに移動するフェールオーバーグループの数です。**[Make Standby]** をクリックします。

ASDM は、セカンダリ ユニット上のフェールオーバー グループ 1 の IP アドレスに自動的に再接続されます。

ステップ 16 **[Monitoring]** > **[Failover]** > **[System]** の順に選択し、**[Reload Standby]** をクリックして、プライマリユニットをリロードします。

ステップ 17 フェールオーバーグループは、[Preempt Enabled] を使用して設定されると、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。ASDM は、プライマリ ユニット上のフェールオーバー グループ 1 の IP アドレスに自動的に再接続されます。

プラットフォームモードでの Firepower 2100 のアップグレード

このドキュメントでは、プラットフォームモードでの Firepower 2100 のスタンドアロンまたはフェールオーバー展開用に、ASA、FXOS、および ASDM のアップグレードを計画し、実装する方法について説明します。バージョン 9.13 以前では、Firepower 2100 はプラットフォームモードのみをサポートしていました。9.14 以降では、アプライアンスモードがデフォルトで

す。9.14 以降では、ASA で **show fxos mode** コマンドを使用して現在のモードを決定します。アプライアンスモードの手順については、アプライアンスモードでの Firepower 1000 および Firepower 2100 のアップグレード （85 ページ） を参照してください。

スタンドアロン ユニットのアップグレード

スタンドアロン ユニットをアップグレードするには FXOS CLI または FirePOWER シャーシ マネージャを使用します。

Firepower Chassis Manager を使用したスタンドアロン ユニットのアップグレード

このセクションでは、スタンドアロン ユニットの ASA バンドルをアップグレードする方法を説明します。管理コンピュータからパッケージをアップロードします。

手順

ステップ 1 Firepower Chassis Manager に接続します。

ステップ 2 **[System]** > **[Updates]** を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。

ステップ 3 [Upload Image] をクリックして管理コンピュータから新しいパッケージをアップロードします。

ステップ 4 [Choose File] をクリックして対象のファイルに移動し、アップロードするパッケージを選択します。

ステップ 5 [Upload] をクリックします。

選択したパッケージがシャーシにアップロードされます。[Upload Image] のダイアログボックスにアップロードの状況が表示されます。[Success] のダイアログボックスが表示されたら [OK] をクリックします。アップロードが完了すると、イメージの整合性が自動的に検証されます。

ステップ 6 新しいパッケージの右側の [Upgrade] アイコンをクリックします。

ステップ 7 [Yes] をクリックして、インストールを続行することを確認します。

新しいパッケージが読み込まれていることを示すインジケータはありません。アップグレードプロセスの開始時には引き続き Firepower Chassis Manager が表示されます。システムのリブート時にログアウトされます。Firepower Chassis Manager にログインするには、システムのリブート完了を待つ必要があります。リブートプロセスには約 20 分かかります。リブート後、ログイン画面が表示されます。

FXOS CLI を使用したスタンドアロン ユニットのアップグレード

このセクションでは、スタンドアロン ユニットの ASA バンドルをアップグレードする方法を説明します。パッケージを FirePOWER 2100 シャーシにコピーするには、FTP、SCP、SFTP、または TFTP を使用できます。

手順

ステップ 1 コンソール ポート（推奨）または SSH を使用して、FXOS CLI に接続します。

ステップ 2 シャーシにパッケージをダウンロードします。

a) ファームウェア モードを入力します。

scope firmware

例：

```
firepower-2110# scope firmware
firepower-2110 /firmware#
```

b) パッケージをダウンロードします。

download image *url*

次のいずれかを使用してインポートするファイルの URL を指定します。

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*

例：

```
firepower-2110 /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
 download progress.
```

c) ダウンロード プロセスをモニタします。

show download-task

例：

```
firepower-2110 /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
firepower-2110 /firmware #
```

ステップ 3 新しいパッケージのダウンロードが終了（[ダウンロード済み（Downloaded）] の状態）したら、パッケージを起動します。

a) 新しいパッケージのバージョン番号を表示します。

show package

例：

```
firepower-2110 /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
firepower-2110 /firmware #
```

b) パッケージをインストールします。

scope auto-install

install security-pack version *version*

show package の出力で、**security-pack version** 番号の **Package-Vers** 値をコピーします。シャーシが ASA イメージをインストールして再起動します。

例：

```
firepower-2110 /firmware # scope auto-install
firepower-2110 /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
firepower-2110 /firmware/auto-install #
```

ステップ 4 シャーシのリブートが完了するのを待ちます（5 ～ 10 分）。

FXOS が起動しても、ASA が稼働するまで（5 分）待機する必要があります。次のメッセージが表示されるまで待機します。

```
firepower-2110#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
```

```
Cisco ASA started successfully.
[…]
```

アクティブ/スタンバイ フェールオーバー ペアのアップグレード

アクティブ/スタンバイ フェールオーバー ペアをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、FXOS CLI または FirePOWER シャーシマネージャを使用します。

Firepower Chassis Manager を使用したアクティブ/スタンバイ フェールオーバー ペアのアップグレード

このセクションでは、アクティブ/スタンバイ フェールオーバー ペアの ASA バンドルをアップグレードする方法を説明します。管理コンピュータからパッケージをアップロードします。

始める前に

アクティブになっているユニットとスタンバイになっているユニットを確認する必要があります。ASDM をアクティブな ASA の IP アドレスに接続します。アクティブ装置は、常にアクティブな IP アドレスを保有しています。次に、**[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** の順に選択して、このユニットの優先順位（プライマリまたはセカンダリ）を表示し、接続先のユニットを確認できるようにします。

手順

ステップ 1 スタンバイ装置をアップグレードします。

a) スタンバイ装置の Firepower Chassis Manager に接続します。

b) **[System]** > **[Updates]** を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。

c) [Upload Image] をクリックして管理コンピュータから新しいパッケージをアップロードします。

d) [Choose File] をクリックして対象のファイルに移動し、アップロードするパッケージを選択します。

e) [Upload] をクリックします。

選択したパッケージがシャーシにアップロードされます。[Upload Image] のダイアログボックスにアップロードの状況が表示されます。[Success] のダイアログボックスが表示されたら [OK] をクリックします。アップロードが完了すると、イメージの整合性が自動的に検証されます。

f) 新しいパッケージの右側の [Upgrade] アイコンをクリックします。

g) [Yes] をクリックして、インストールを続行することを確認します。

新しいパッケージが読み込まれていることを示すインジケータはありません。アップグレード プロセスの開始時には引き続き Firepower Chassis Manager が表示されます。システムのリブート時にログアウトされます。Firepower Chassis Manager にログインするには、

システムのリブート完了を待つ必要があります。リブートプロセスには約 20 分かかります。リブート後、ログイン画面が表示されます。

ステップ 2 アップグレードした装置をアクティブ装置にして、アップグレード済みの装置にトラフィックが流れるようにします。

a) スタンバイ ASA IP アドレスに接続して、スタンバイ装置で ASDM を起動します。

b) **[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** の順に選択し、[Make Active] をクリックして、スタンバイ装置を強制的にアクティブにします。

ステップ 3 以前のアクティブ装置をアップグレードします。

a) 以前のアクティブ装置の Firepower Chassis Manager に接続します。

b) **[System]** > **[Updates]** を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。

c) [Upload Image] をクリックして管理コンピュータから新しいパッケージをアップロードします。

d) [Choose File] をクリックして対象のファイルに移動し、アップロードするパッケージを選択します。

e) [Upload] をクリックします。

選択したパッケージがシャーシにアップロードされます。[Upload Image] のダイアログボックスにアップロードの状況が表示されます。[成功（Success）] のダイアログボックスが表示されたら [OK] をクリックします。アップロードが完了すると、イメージの整合性が自動的に検証されます。

f) 新しいパッケージの右側の [アップグレード（Upgrade）] アイコンをクリックします。

g) [はい（Yes）] をクリックして、インストールを続行することを確認します。

新しいパッケージが読み込まれていることを示すインジケータはありません。アップグレード プロセスの開始時には引き続き Firepower Chassis Manager が表示されます。システムのリブート時にログアウトされます。Firepower Chassis Manager にログインするには、システムのリブート完了を待つ必要があります。リブートプロセスには約 20 分かかります。リブート後、ログイン画面が表示されます。

FXOS CLI を使用したアクティブ/スタンバイ フェールオーバー ペアのアップグレード

このセクションでは、アクティブ/スタンバイ フェールオーバー ペアの ASA バンドルをアップグレードする方法を説明します。パッケージを FirePOWER 2100 シャーシにコピーするには、FTP、SCP、SFTP、または TFTP を使用できます。

始める前に

アクティブになっているユニットとスタンバイになっているユニットを確認する必要があります。フェールオーバー ステータスを確認するには、ASA プロンプトを調べます。フェールオーバー ステータスと優先順位（プライマリまたはセカンダリ）を表示するように ASA プロンプトを設定できます。これは、接続しているユニットを特定するのに役立ちます。prompt コマン

ドを参照してください。ただし、FXOS プロンプトでは ASA フェールオーバーは認識されません。代わりに、ASA **show failover** コマンドを入力して、このユニットのステータスと優先順位（プライマリまたはセカンダリ）を表示します。

手順

ステップ 1 スタンバイ装置をアップグレードします。

a) コンソール ポート（推奨）または SSH を使用して、スタンバイ装置の FXOS CLI に接続します。

b) ファームウェア モードを入力します。

scope firmware

例：

```
2110-sec# scope firmware
2110-sec /firmware#
```

c) パッケージをダウンロードします。

download image *url*

次のいずれかを使用してインポートするファイルの URL を指定します。

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*

例：

```
2110-sec /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
 download progress.
```

d) ダウンロード プロセスをモニタします。

show download-task

例：

```
2110-sec /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181            0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181            0                 Downloading
```

```
2110-sec /firmware #
```

e) 新しいパッケージのダウンロードが終了（[ダウンロード済み（Downloaded）] の状態）したら、パッケージを起動します。新しいパッケージのバージョン番号を表示します。

show package

例：

```
2110-sec /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
2110-sec /firmware #
```

f) パッケージをインストールします。

scope auto-install

install security-pack version *version*

show package の出力で、**security-pack version** 番号の **Package-Vers** 値をコピーします。シャーシが ASA イメージをインストールして再起動します。

例：

```
2110-sec /firmware # scope auto-install
2110-sec /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-sec /firmware/auto-install #
```

g) シャーシのリブートが完了するのを待ちます（5 ～ 10 分）。

FXOS が起動しても、ASA が稼働するまで（5 分）待機する必要があります。次のメッセージが表示されるまで待機します。

```
2110-sec#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
```

```
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

ステップ 2 アップグレードした装置をアクティブ装置にして、アップグレード済みの装置にトラフィックが流れるようにします。

a) FXOS からスタンバイ ASA CLI に接続します。

connect asa

enable

デフォルトで、イネーブル パスワードは空白です。

例：

```
2110-sec# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
asa/stby/sec> enable
Password: <blank>
asa/stby/sec#
```

b) スタンバイ装置を強制的にアクティブにします。

failover active

例：

```
asa/stby/sec> failover active
asa/act/sec#
```

c) FXOS コンソールに戻るには、**Ctrl+a**、**d** と入力します。

ステップ 3 以前のアクティブ装置をアップグレードします。

a) コンソール ポート（推奨）または SSH を使用して、以前のアクティブ装置の FXOS CLI に接続します。

b) ファームウェア モードを入力します。

scope firmware

例：

```
2110-pri# scope firmware
2110-pri /firmware#
```

c) パッケージをダウンロードします。

download image *url*

次のいずれかを使用してインポートするファイルの URL を指定します。

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*

例：

```
2110-pri /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
 download progress.
```

d) ダウンロード プロセスをモニタします。

show download-task

例：

```
2110-pri /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
2110-pri /firmware #
```

e) 新しいパッケージのダウンロードが終了（[ダウンロード済み（Downloaded）] の状態）したら、パッケージを起動します。新しいパッケージのバージョン番号を表示します。

show package

例：

```
2110-pri /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
2110-pri /firmware #
```

f) パッケージをインストールします。

scope auto-install

install security-pack version *version*

show package の出力で、**security-pack version** 番号の **Package-Vers** 値をコピーします。シャーシが ASA イメージをインストールして再起動します。

例：

```
2110-pri /firmware # scope auto-install
2110-pri /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-pri /firmware/auto-install #
```

g) シャーシのリブートが完了するのを待ちます（5 ～ 10 分）。

FXOS が起動しても、ASA が稼働するまで（5 分）待機する必要があります。次のメッセージが表示されるまで待機します。

```
2110-pri#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

アクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー ペアをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、FXOS CLI または FirePOWER シャーシマネージャを使用します。

Firepower Chassis Manager を使用したアクティブ/アクティブ フェールオーバー ペアのアップグレード

このセクションでは、アクティブ/アクティブ フェールオーバー ペアの ASA バンドルをアップグレードする方法を説明します。管理コンピュータからパッケージをアップロードします。

手順

ステップ 1 プライマリ ユニットの両方のフェールオーバー グループをアクティブにします。

a) フェールオーバー グループ 1 の管理アドレスに接続して、プライマリ ユニット（またはフェールオーバー グループ 1 がアクティブに設定されているユニット）で ASDM を起動します。

b) **[モニタリング（Monitoring）] > [フェールオーバー（Failover）] > [フェールオーバー グループ 2（Failover Group 2）]** の順に選択して、[アクティブにする（Make Active）] をクリックします。

c) 後続の手順のために、このユニットの ASDM に接続したままにします。

ステップ 2 セカンダリ ユニットをアップグレードします。

a) セカンダリ ユニットの Firepower Chassis Manager に接続します。

b) **[System] > [Updates]** を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。

c) [Upload Image] をクリックして管理コンピュータから新しいパッケージをアップロードします。

d) [Choose File] をクリックして対象のファイルに移動し、アップロードするパッケージを選択します。

e) [Upload] をクリックします。

選択したパッケージがシャーシにアップロードされます。[Upload Image] のダイアログボックスにアップロードの状況が表示されます。[Success] のダイアログボックスが表示されたら [OK] をクリックします。アップロードが完了すると、イメージの整合性が自動的に検証されます。

f) 新しいパッケージの右側の [Upgrade] アイコンをクリックします。

g) [Yes] をクリックして、インストールを続行することを確認します。

新しいパッケージが読み込まれていることを示すインジケータはありません。アップグレード プロセスの開始時には引き続き Firepower Chassis Manager が表示されます。システムのリブート時にログアウトされます。Firepower Chassis Manager にログインするには、システムのリブート完了を待つ必要があります。リブートプロセスには約 20 分かかります。リブート後、ログイン画面が表示されます。

ステップ 3 セカンダリ ユニットの両方のフェールオーバー グループをアクティブにします。プライマリ ユニットの ASDM で、**[Monitoring] > [Failover] > [Failover Group 1]** の順に選択して、[Make Standby] をクリックします。

ASDM は、セカンダリ ユニット上のフェールオーバー グループ 1 の IP アドレスに自動的に再接続されます。

ステップ 4 プライマリ ユニットをアップグレードします。

a) プライマリ ユニットの Firepower Chassis Manager に接続します。

b) **[System] > [Updates]** を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。

c) [Upload Image] をクリックして管理コンピュータから新しいパッケージをアップロードします。
d) [Choose File] をクリックして対象のファイルに移動し、アップロードするパッケージを選択します。
e) [Upload] をクリックします。

選択したパッケージがシャーシにアップロードされます。[Upload Image] のダイアログボックスにアップロードの状況が表示されます。[成功（Success）] のダイアログボックスが表示されたら [OK] をクリックします。アップロードが完了すると、イメージの整合性が自動的に検証されます。

f) 新しいパッケージの右側の [アップグレード（Upgrade）] アイコンをクリックします。
g) [はい（Yes）] をクリックして、インストールを続行することを確認します。

新しいパッケージが読み込まれていることを示すインジケータはありません。アップグレード プロセスの開始時には引き続き Firepower Chassis Manager が表示されます。システムのリブート時にログアウトされます。Firepower Chassis Manager にログインするには、システムのリブート完了を待つ必要があります。リブートプロセスには約 20 分かかります。リブート後、ログイン画面が表示されます。

ステップ 5 フェールオーバー グループは、[Preempt Enabled] を使用して設定されると、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。[Preempt Enabled] でフェールオーバー グループが設定されていない場合は、[Monitoring] > [Failover] > [Failover Group #] ペインを使用して、指定された装置上でアクティブ ステータスに戻すことができます。

FXOS CLI を使用したアクティブ/アクティブ フェールオーバー ペアのアップグレード

このセクションでは、アクティブ/アクティブ フェールオーバー ペアの ASA バンドルをアップグレードする方法を説明します。パッケージを FirePOWER 2100 シャーシにコピーするには、FTP、SCP、SFTP、または TFTP を使用できます。

手順

ステップ 1 コンソール ポート（推奨）または SSH を使用して、セカンダリ ユニットの FXOS CLI に接続します。

ステップ 2 プライマリ ユニットの両方のフェールオーバー グループをアクティブにします。

a) FXOS から ASA CLI に接続します。

connect asa

enable

デフォルトで、イネーブル パスワードは空白です。

例：

```
2110-sec# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
```

```
Type help or '?' for a list of available commands.
asa/act/sec> enable
Password: <blank>
asa/act/sec#
```

b) プライマリ ユニットの両方のフェールオーバー グループをアクティブにします。

no failover active group 1

no failover active group 2

例：

```
asa/act/sec# no failover active group 1
asa/act/sec# no failover active group 2
```

c) **Ctrl + a**、**d** を押下し、FXOS コンソールに戻ります。

ステップ 3 セカンダリ ユニットをアップグレードします。

a) FXOS で、ファームウェア モードに入ります。

scope firmware

例：

```
2110-sec# scope firmware
2110-sec /firmware#
```

b) パッケージをダウンロードします。

download image *url*

次のいずれかを使用してインポートするファイルの URL を指定します。

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*

例：

```
2110-sec /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
 download progress.
```

c) ダウンロード プロセスをモニタします。

show download-task

例：

```
2110-sec /firmware # show download

Download task:
```

```
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
2110-sec /firmware #
```

d) 新しいパッケージのダウンロードが終了（[ダウンロード済み（Downloaded）] の状態）したら、パッケージを起動します。新しいパッケージのバージョン番号を表示します。

show package

例：

```
2110-sec /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
2110-sec /firmware #
```

e) パッケージをインストールします。

scope auto-install

install security-pack version *version*

show package の出力で、**security-pack version** 番号の **Package-Vers** 値をコピーします。シャーシが ASA イメージをインストールして再起動します。

例：

```
2110-sec /firmware # scope auto-install
2110-sec /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-sec /firmware/auto-install #
```

f) シャーシのリブートが完了するのを待ちます（5 ～ 10 分）。

FXOSが起動しても、ASAが稼働するまで（5分）待機する必要があります。次のメッセージが表示されるまで待機します。

```
2110-sec#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

ステップ 4 セカンダリ ユニットの両方のフェールオーバー グループをアクティブにします。

a) FXOS から ASA CLI に接続します。

connect asa

enable

デフォルトで、イネーブル パスワードは空白です。

例：

```
2110-sec# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
asa/stby/sec> enable
Password: <blank>
asa/stby/sec#
```

b) セカンダリ ユニットの両方のフェールオーバー グループをアクティブにします。

failover active group 1

failover active group 2

例：

```
asa/stby/sec# failover active group 1
asa/act/sec# failover active group 2
```

c) **Ctrl + a**、**d** を押下し、FXOS コンソールに戻ります。

ステップ 5 プライマリ ユニットをアップグレードします。

a) コンソール ポート（推奨）または SSH を使用して、プライマリ ユニットの FXOS CLI に接続します。

b) ファームウェア モードを入力します。

scope firmware

例：

```
2110-pri# scope firmware
```

```
2110-pri /firmware#
```

c) パッケージをダウンロードします。

download image *url*

次のいずれかを使用してインポートするファイルの URL を指定します。

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*

例：

```
2110-pri /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
 download progress.
```

d) ダウンロード プロセスをモニタします。

show download-task

例：

```
2110-pri /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
2110-pri /firmware #
```

e) 新しいパッケージのダウンロードが終了（[ダウンロード済み（Downloaded）] の状態）したら、パッケージを起動します。新しいパッケージのバージョン番号を表示します。

show package

例：

```
2110-pri /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
2110-pri /firmware #
```

f) パッケージをインストールします。

scope auto-install

install security-pack version *version*

show package の出力で、**security-pack version** 番号の **Package-Vers** 値をコピーします。シャーシが ASA イメージをインストールして再起動します。

例：

```
2110-pri /firmware # scope auto-install
2110-pri /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-pri /firmware/auto-install #
```

g) シャーシのリブートが完了するのを待ちます（5 ～ 10 分）。

FXOS が起動しても、ASA が稼働するまで（5 分）待機する必要があります。次のメッセージが表示されるまで待機します。

```
2110-pri#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

ステップ 6 フェールオーバー グループは、ASA **preempt** コマンドを使用して設定されている場合、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。フェールオーバーグループが **preempt** コマンドによって設定されていない場合は、ASA CLI に接続し、**failover active group**コマンドを使用して、指定された装置でそれらのステータスをアクティブに戻すことができます。

ASA 5500-X、ASAv、ASASM、ISA 3000 のアップグレード

このドキュメントでは、スタンドアロン、フェールオーバー、またはクラスタリング導入用に ASA 5500-X、ASAv、ASASM、または ISA 3000 の ASA および ASDM アップグレードを計画し、実装する方法について説明します。

スタンドアロン ユニットのアップグレード

スタンドアロン ユニットをアップグレードするには CLI または ASDM を使用します。

CLI を使用したスタンドアロン ユニットのアップグレード

ここでは、ASDMイメージおよびASAイメージをインストールする方法について説明します。また、ASA FirePower モジュールをアップグレードするタイミングについても説明します。

始める前に

この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバタイプについては、『ASA Command Reference』の **copy** コマンドを参照してください。

手順

ステップ 1 特権 EXEC モードで、ASA ソフトウェアをフラッシュメモリにコピーします。

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

例：

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asa-9-12-1-smp-k8.bin
disk0:/asa-9-12-1-smp-k8.bin
```

ステップ 2 ASDM イメージをフラッシュメモリにコピーします。

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

例：

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-7121.bin disk0:/asdm-7121.bin
```

ステップ 3 グローバル コンフィギュレーション モードにアクセスします。

configure terminal

例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

ステップ 4 設定されている現在のブート イメージを表示します（最大 4 個）。

show running-config boot system

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。

例：

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ステップ 5 既存のブートイメージコンフィギュレーションがある場合は削除します。新しいブートイメージを最初の選択肢として入力できるようにするためです。

no boot system disk*n***:/**[*path*/]*asa_image_name*

例：

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa931-smp-k8.bin
```

ステップ 6 ブートする ASA イメージを設定します（先ほどアップロードしたもの）。

boot system disk*n***:/**[*path*/]*asa_image_name*

このイメージが使用できない場合に使用するバックアップイメージに対して、このコマンドを繰り返します。たとえば、先ほど削除したイメージを再入力できます。

例：

```
ciscoasa(config)# boot system disk0:/asa-9-12-1-smp-k8.bin
```

ステップ 7 使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

asdm image disk*n***:/**[*path*/]*asdm_image_name*

使用するように設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

例：

```
ciscoasa(config)# asdm image disk0:/asdm-7121.bin
```

ステップ 8 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

ステップ 9 ASA をリロードします。

reload

ステップ 10 ASA FirePOWER モジュールをアップグレードする場合は、ASA REST API を無効にします。無効にしない場合アップグレードは失敗します。

no rest-api agent

次のコマンドを実行して、アップグレード後に REST API を再度有効にすることができます。

rest-api agent

（注） FirePOWER モジュールのバージョン 6.0 以降を実行している場合、ASA 5506-X シリーズは ASA の REST API をサポートしません。

ステップ 11 ASA FirePOWER モジュールをアップグレードします。

ASDM を使用した、ローカル コンピュータからのスタンドアロン ユニットのアップグレード

Upgrade Software from Local Computer ツールにより、コンピュータからフラッシュファイルシステムにイメージファイルをアップロードし、ASA をアップグレードできます。

手順

ステップ 1 メイン ASDM アプリケーション ウィンドウで、**[ツール（Tools）]** > **[Upgrade Software from Local Computer]** の順に選択します。

[ソフトウェアのアップグレード（Upgrade Software）] ダイアログボックスが表示されます。

ステップ 2 [アップロードするイメージ（Image to Upload）] ドロップダウンリストから、[ASDM] を選択します。

ステップ 3 [ローカル ファイルのパス（Local File Path）] フィールドで [ローカル ファイルを参照（Browse Local Files）] をクリックして PC 上のファイルを見つけます。

ステップ 4 [フラッシュ ファイル システムのパス（Flash File System Path）] フィールドで [フラッシュを参照（Browse Flash）] をクリックしてフラッシュ ファイル システム上のディレクトリまたはファイルを見つけます。

ステップ 5 [Upload Image] をクリックします。

アップグレード プロセスには数分かかる場合があります。

ステップ 6 このイメージを ASDM イメージとして設定するように求められます。[Yes] をクリックします。

ステップ 7 ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。

アップグレード ツールを終了します。**注**：ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM を終了して再接続します。

ステップ 8 これらの手順を繰り返し、[アップロードするイメージ（Image to Upload）] ドロップダウンリストで [ASA] を選択します。この手順は、その他のタイプのファイルのアップロードでも同じです。

ステップ 9 **[Tools]** > **[System Reload]** を選択して、ASA をリロードします。

リロードの詳細の確認を求める新しいウィンドウが表示されます。

a) [Save the running configuration at the time of reload] オプション ボタン（デフォルト）をクリックします。
b) リロードする時刻を選択します（たとえば、デフォルトの [Now]）。
c) [Schedule Reload] をクリックします。

リロードが開始されると、[Reload Status] ウィンドウにリロードの進行状況が表示されます。ASDM を終了するオプションも表示されます。

ステップ 10 ASA のリロード後、ASDM を再起動します。

コンソールポートでリロードの状況を確認できます。または、数分待った後に ASDM を使用して、接続可能になるまで再試行することもできます。

ステップ 11 ASA FirePOWER モジュールをアップグレードする場合は、**[Tools]** > **[コマンドライン インターフェイス（Command Line Interface）]** を選択し、**no rest-api agent** を入力して ASA REST API を無効にします。

REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。次のコマンドを実行して、アップグレード後に REST API を再度有効にすることができます。

rest-api agent

（注） FirePOWER モジュールのバージョン 6.0 以降を実行している場合、ASA 5506-X シリーズは ASA の REST API をサポートしません。

ステップ 12 ASA FirePOWER モジュールをアップグレードします。

ASDM Cisco.com ウィザードを使用したスタンドアロンユニットのアップグレード

Upgrade Software from Cisco.com Wizard により、ASDM および ASA を最新のバージョンに自動的にアップグレードできます。

このウィザードでは、次の操作を実行できます。

- アップグレード用の ASA イメージ ファイルまたは ASDM イメージ ファイルを選択する。

（注） ASDM は最新のイメージバージョンをダウンロードし、そこにはビルド番号が含まれています。たとえば、9.9(1) をダウンロードする場合に、ダウンロードが 9.9(1.2) となる可能性があります。この動作は想定されているため、計画したアップグレードを続行できます。

- 実行したアップグレードの変更点を確認する。
- イメージをダウンロードし、インストールする。
- インストールのステータスを確認する。
- インストールが正常に完了した場合は、ASA をリロードして、コンフィギュレーションを保存し、アップグレードを完了する。

始める前に

内部的な変更により、このウィザードでは ASDM 7.10(1) 以降の使用のみがサポートされています。また、イメージの命名が変更されたため、ASA 9.10(1) 以降にアップグレードするには、ASDM 7.12(1) 以降を使用する必要があります。ASDM は ASA の以前のリリースと下位互換性があるため、実行している ASA バージョンを問わず、ASDM をアップグレードすることができます。

手順

ステップ 1 **[Tools]** > **[Check for ASA/ASDM Updates]** を選択します。

マルチコンテキストモードでは、システムからこのメニューにアクセスします。

[Cisco.com Authentication] ダイアログボックスが表示されます。

ステップ 2 Cisco.com のユーザ ID とパスワードを入力して、[Login] をクリックします。

[Cisco.com Upgrade Wizard] が表示されます。

（注） 利用可能なアップグレードがない場合は、ダイアログボックスが表示されます。ウィザードを終了するには、[OK] をクリックします。

ステップ 3 [Next] をクリックして [Select Software] 画面を表示します。

現在の ASA バージョンおよび ASDM バージョンが表示されます。

ステップ 4 ASA バージョンおよび ASDM バージョンをアップグレードするには、次の手順を実行します。

a) [ASA] 領域で、[Upgrade to] チェックボックスをオンにしてから、アップグレードする ASA バージョンをドロップダウン リストから選択します。

b) [ASDM] 領域で、[Upgrade to] チェックボックスをオンにしてから、アップグレードする ASDM バージョンをドロップダウン リストから選択します。

ステップ 5 [Next] をクリックして [Review Changes] 画面を表示します。

ステップ 6 次の項目を確認します。

- ダウンロードした ASA イメージ ファイルや ASDM イメージ ファイルが正しいファイルであること。
- アップロードする ASA イメージ ファイルや ASDM イメージ ファイルが正しいファイルであること。

- 正しい ASA ブート イメージが選択されていること。

ステップ 7 [Next] をクリックして、アップグレード インストールを開始します。

アップグレード インストールの進行状況を示すステータスを表示できます。

[Results] 画面が表示され、アップグレードインストール ステータス（成功または失敗）など、追加の詳細が示されます。

ステップ 8 アップグレード インストールが成功した場合に、アップグレード バージョンを有効にするには、[Save configuration and reload device now] チェックボックスをオンにして、ASA を再起動し、ASDM を再起動します。

ステップ 9 [Finish] をクリックして、ウィザードを終了し、コンフィギュレーションに対して行った変更を保存します。

（注） 次に高いバージョン（存在する場合）にアップグレードするには、ウィザードを再起動する必要があります。

ステップ 10 ASA のリロード後、ASDM を再起動します。

コンソールポートでリロードの状況を確認できます。または、数分待った後に ASDM を使用して、接続可能になるまで再試行することもできます。

ステップ 11 ASA FirePOWER モジュールをアップグレードする場合は、**[Tools]** > **[Command Line Interface]** を選択し、**no rest-api agent** を入力して ASA REST API を無効にします。

REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。次のコマンドを実行して、アップグレード後に REST API を再度有効にすることができます。

rest-api agent

（注） FirePOWER モジュールのバージョン 6.0 以降を実行している場合、ASA 5506-X シリーズは ASA の REST API をサポートしません。

ステップ 12 ASA FirePOWER モジュールをアップグレードします。

アクティブ/スタンバイ フェールオーバー ペアのアップグレード

アクティブ/スタンバイ フェールオーバー ペアをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、CLI または ASDM を使用します。

CLI を使用したアクティブ/スタンバイ フェールオーバー ペアのアップグレード

アクティブ/スタンバイ フェールオーバー ペアをアップグレードするには、次の手順を実行します。

始める前に

- アクティブ装置で次の手順を実行します。SSH アクセスの場合、アクティブな IP アドレスに接続します。アクティブ装置は常にこの IP アドレスを保有しています。CLI に接続する場合は、ASA プロンプトを調べてフェールオーバー ステータスを確認します。フェールオーバー ステータスと優先順位（プライマリまたはセカンダリ）を表示するように ASA プロンプトを設定できます。これは、接続しているユニットを特定するのに役立ちます。prompt コマンドを参照してください。代わりに、**show failover** コマンドを入力して、このユニットのステータスと優先順位（プライマリまたはセカンダリ）を表示します。
- この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバタイプについては、『ASA Command Reference』の **copy** コマンドを参照してください。

手順

ステップ 1 特権 EXEC モード時にアクティブ装置で、ASA ソフトウェアをアクティブ装置のフラッシュ メモリにコピーします。

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]/*asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

例：

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin
disk0:/asa9-15-1-smp-k8.bin
```

ステップ 2 ソフトウェアをスタンバイ装置にコピーします。アクティブ装置で指定したのと同じパスを指定してください。

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]/*asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

例：

```
asa/act# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin disk0:/asa9-15-1-smp-k8.bin
```

ステップ 3 ASDM イメージをアクティブ装置のフラッシュ メモリにコピーします。

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]/*asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

例：

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-77171417151.bin
disk0:/asdm-77171417151.bin
```

ステップ 4 ASDMイメージをスタンバイ装置にコピーします。アクティブ装置で指定したのと同じパスを指定してください。

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]/*asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

例：

```
asa/act# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asdm-77171417151.bin disk0:/asdm-77171417151.bin
```

ステップ 5 まだグローバル コンフィギュレーション モードを開始していない場合は、グローバル コンフィギュレーション モードを開始します。

configure terminal

ステップ 6 設定されている現在のブート イメージを表示します（最大 4 個）。

show running-config boot system

例：

```
asa/act(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。

ステップ 7 既存のブートイメージコンフィギュレーションがある場合は削除します。新しいブートイメージを最初の選択肢として入力できるようにするためです。

no boot system disk*n***:/**[*path*/]*asa_image_name*

例：

```
asa/act(config)# no boot system disk0:/cdisk.bin
asa/act(config)# no boot system disk0:/asa931-smp-k8.bin
```

ステップ 8 ブートする ASA イメージを設定します（先ほどアップロードしたもの）。

boot system disk*n***:/**[*path*/]*asa_image_name*

例：

```
asa/act(config)# boot system disk0://asa9-15-1-smp-k8.bin
```

このイメージが使用できない場合に使用するバックアップイメージに対して、このコマンドを繰り返します。たとえば、先ほど削除したイメージを再入力できます。

ステップ 9 使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

asdm image disk*n***:/**[*path*/]*asdm_image_name*

例：

```
asa/act(config)# asdm image disk0:/asdm-77171417151.bin
```

使用するように設定できるASDMイメージは1つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

ステップ 10 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

これらの設定変更は、スタンバイ ユニットに自動的に保存されます。

ステップ 11 ASA FirePOWER モジュールをアップグレードする場合は、ASA REST API を無効にします。無効にしない場合アップグレードは失敗します。

no rest-api agent

ステップ 12 スタンバイ装置の ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をスタンバイ管理 IP アドレスに接続します。アップグレードが完了するまで待ちます。

ステップ 13 スタンバイ装置をリロードして新しいイメージを起動します。

failover reload-standby

スタンバイ装置のロードが完了するまで待ちます。**show failover** コマンドを使用して、スタンバイ ユニットが Standby Ready 状態かどうかを検証します。

ステップ 14 強制的にアクティブ装置からスタンバイ装置へのフェールオーバーを行います。

no failover active

SSH セッションから切断されている場合は、新しいアクティブ/元のスタンバイ ユニット上に現在あるメイン IP アドレスに再接続します。

ステップ 15 以前のアクティブ装置の ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をスタンバイ管理 IP アドレスに接続します。アップグレードが完了するまで待ちます。

ステップ 16 新しいアクティブ装置から、元のアクティブ装置（今の新しいスタンバイ装置）をリロードします。

failover reload-standby

例：

```
asa/act# failover reload-standby
```

（注） 元のアクティブ ユニットのコンソール ポートに接続されている場合は、代わりに **reload** コマンドを入力して、元のアクティブ ユニットをリロードする必要があります。

ASDM を使用したアクティブ/スタンバイ フェールオーバー ペアのアップグレード

アクティブ/スタンバイ フェールオーバー ペアをアップグレードするには、次の手順を実行します。

始める前に

ローカル管理コンピュータに ASA と ASDM のイメージを配置します。

手順

ステップ 1 スタンバイ IP アドレスに接続して、*standby* ユニット上で ASDM を起動します。

ステップ 2 メイン ASDM アプリケーション ウィンドウで、**[ツール（Tools）] > [Upgrade Software from Local Computer]** の順に選択します。

[ソフトウェアのアップグレード（Upgrade Software）] ダイアログボックスが表示されます。

ステップ 3 [アップロードするイメージ（Image to Upload）] ドロップダウンリストから、[ASDM] を選択します。

ステップ 4 [Local File Path] フィールドにコンピュータ上のファイルへのローカル パスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを見つけます。

ステップ 5 [フラッシュファイルシステムのパス（Flash File System Path）] フィールドにフラッシュファイルシステムへのパスを入力するか、[フラッシュの参照（Browse Flash）] をクリックしてフラッシュファイルシステム上のディレクトリまたはファイルを検索します。

ステップ 6 [Upload Image] をクリックします。アップグレード プロセスには数分かかる場合があります。

このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。

ステップ 7 これらの手順を繰り返し、[Image to Upload] ドロップダウン リストで [ASA] を選択します。

このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。

ステップ 8 メイン IP アドレスに接続して ASDM をアクティブなユニットに接続し、スタンバイ ユニットで使用したのと同じファイルの場所を使用して、ASDM ソフトウェアをアップロードします。

ステップ 9 このイメージを ASDM イメージとして設定するように求められたら、[Yes] をクリックします。

ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。アップグレード ツールを終了します。**注**：ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM をリロードします。

ステップ 10 スタンバイ ユニットで使用したのと同じファイルの場所を使用して、ASA ソフトウェアをアップロードします。

ステップ 11 このイメージを ASA イメージとして設定するように求められたら、[Yes] をクリックします。

新しいイメージを使用するために、ASA をリロードするよう求められます。[OK] をクリックします。アップグレード ツールを終了します。

ステップ 12 コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。

これらの設定変更は、スタンバイ ユニットに自動的に保存されます。

ステップ 13 ASA FirePOWER モジュールをアップグレードする場合は、**[ツール（Tools）]** > **[コマンドラインインターフェイス（Command Line Interface）]** を選択し、**no rest-api enable** を入力して ASA REST API を無効にします。

REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。

ステップ 14 スタンバイ装置の ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をスタンバイ管理 IP アドレスに接続します。アップグレードの完了を待ってから、ASDM をアクティブ装置に接続します。

ステップ 15 **[モニタリング（Monitoring）]** > **[プロパティ（Properties）]** > **[フェールオーバー（Failover）]** > **[ステータス（Status）]** の順に選択し、[スタンバイのリロード（Reload Standby）] をクリックして、スタンバイ装置をリロードします。

[System] ペインを開いたまま、スタンバイ ユニットがリロードされるのを確認します。

ステップ 16 スタンバイ ユニットがリロードしたら、**[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** の順に選択し、[Make Standby] をクリックして、アクティブなユニットをスタンバイ ユニットにフェールオーバーします。

ASDM は新しいアクティブ ユニットに自動的に再接続されます。

ステップ 17 以前のアクティブ装置の ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をスタンバイ管理 IP アドレスに接続します。アップグレードの完了を待ってから、ASDM をアクティブ装置に接続します。

ステップ 18 **[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** の順に選択し、[Reload Standby] をクリックして、（新しい）スタンバイ ユニットをリロードします。

アクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー ペアをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、CLI または ASDM を使用します。

CLI を使用したアクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー コンフィギュレーションの 2 つの装置をアップグレードするには、次の手順を実行します。

始める前に

- 標準出荷単位で次の手順を実行します。
- これらの手順をシステム実行スペースで実行します。
- この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバタイプについては、『ASA Command Reference』の **copy** コマンドを参照してください。

手順

ステップ 1 特権 EXEC モード時にプライマリ ユニットで、ASA ソフトウェアをフラッシュ メモリにコピーします。

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

例：

```
asa/act/pri# copy ftp://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin
disk0:/asa9-15-1-smp-k8.bin
```

ステップ 2 ソフトウェアをセカンダリ装置にコピーします。プライマリ装置で指定したのと同じパスを指定してください。

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

例：

```
asa/act/pri# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin disk0:/asa9-15-1-smp-k8.bin
```

ステップ 3 ASDM イメージをプライマリ装置のフラッシュ メモリにコピーします。

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

例：

```
asa/act/pri# ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-77171417151.bin
disk0:/asdm-77171417151.bin
```

ステップ 4 ASDMイメージをセカンダリ装置にコピーします。標準出荷単位で指定したのと同じパスを指定してください。

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

例：

```
asa/act/pri# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asdm-77171417151.bin disk0:/asdm-77171417151.bin
```

ステップ 5 まだグローバル コンフィギュレーション モードを開始していない場合は、グローバル コンフィギュレーション モードを開始します。

configure terminal

ステップ 6 設定されている現在のブート イメージを表示します（最大 4 個）。

show running-config boot system

例：

```
asa/act/pri(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。

ステップ 7 既存のブートイメージコンフィギュレーションがある場合は削除します。新しいブートイメージを最初の選択肢として入力できるようにするためです。

no boot system disk*n***:/**[*path*/]*asa_image_name*

例：

```
asa/act/pri(config)# no boot system disk0:/cdisk.bin
asa/act/pri(config)# no boot system disk0:/asa931-smp-k8.bin
```

ステップ 8 ブートする ASA イメージを設定します（先ほどアップロードしたもの）。

boot system disk*n***:/**[*path*/]*asa_image_name*

例：

```
asa/act/pri(config)# boot system disk0://asa9-15-1-smp-k8.bin
```

このイメージが使用できない場合に使用するバックアップイメージに対して、このコマンドを繰り返します。たとえば、先ほど削除したイメージを再入力できます。

ステップ 9 使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

asdm image disk*n***:/**[*path*/]*asdm_image_name*

例：

```
asa/act/pri(config)# asdm image disk0:/asdm-77171417151.bin
```

使用するように設定できるASDMイメージは1つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

ステップ 10 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

これらの設定変更は、セカンダリ ユニットに自動的に保存されます。

ステップ 11 ASA FirePOWER モジュールをアップグレードする場合は、ASA REST API を無効にします。無効にしない場合アップグレードは失敗します。

no rest-api agent

ステップ 12 プライマリ装置の両方のフェールオーバー グループをアクティブにします。

failover active group 1

failover active group 2

例：

```
asa/act/pri(config)# failover active group 1
asa/act/pri(config)# failover active group 2
```

ステップ 13 セカンダリ ユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をフェールオーバー グループ 1 または 2 のスタンバイ管理 IP アドレスに接続します。アップグレードが完了するまで待ちます。

ステップ 14 セカンダリ装置をリロードして新しいイメージを起動します。

failover reload-standby

セカンダリ装置のロードが完了するまで待ちます。**show failover** コマンドを使用して、両方のフェールオーバー グループが Standby Ready 状態であることを確認します。

ステップ 15 セカンダリ装置で、両方のフェールオーバー グループを強制的にアクティブにします。

no failover active group 1

no failover active group 2

例：

```
asa/act/pri(config)# no failover active group 1
asa/act/pri(config)# no failover active group 2
asa/stby/pri(config)#
```

SSH セッションから切断されている場合は、セカンダリ ユニット上に現在あるフェールオーバー グループ 1 の IP アドレスに再接続します。

ステップ 16 プライマリ ユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をフェールオーバー グループ 1 または 2 のスタンバイ管理 IP アドレスに接続します。アップグレードが完了するまで待ちます。

ステップ 17 プライマリ装置をリロードします。

failover reload-standby

例：

```
asa/act/sec# failover reload-standby
```

（注） プライマリ ユニットのコンソール ポートに接続されている場合は、代わりに **reload** コマンドを入力して、プライマリ ユニットをリロードする必要があります。

SSH セッションから切断される場合があります。

ステップ 18 フェールオーバー グループは、**preempt** コマンドを使用して設定されている場合、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。

ASDM を使用したアクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー コンフィギュレーションの 2 つの装置をアップグレードするには、次の手順を実行します。

始める前に

- これらの手順をシステム実行スペースで実行します。
- ローカル管理コンピュータに ASA と ASDM のイメージを配置します。

手順

ステップ 1 フェールオーバー グループ 2 の管理アドレスに接続して、セカンダリ ユニットで ASDM を起動します。

ステップ 2 メイン ASDM アプリケーション ウィンドウで、**[ツール（Tools）]** > **[Upgrade Software from Local Computer]** の順に選択します。

[ソフトウェアのアップグレード（Upgrade Software）] ダイアログボックスが表示されます。

ステップ 3 [アップロードするイメージ（Image to Upload）] ドロップダウンリストから、[ASDM] を選択します。

ステップ 4 [Local File Path] フィールドにコンピュータ上のファイルへのローカル パスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを見つけます。

ステップ 5 [フラッシュファイルシステムのパス（Flash File System Path）] フィールドにフラッシュファイルシステムへのパスを入力するか、[フラッシュの参照（Browse Flash）] をクリックしてフラッシュファイルシステム上のディレクトリまたはファイルを検索します。

ステップ 6 [Upload Image] をクリックします。アップグレード プロセスには数分かかる場合があります。

このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。

ステップ 7 これらの手順を繰り返し、[Image to Upload] ドロップダウン リストで [ASA] を選択します。

このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。

ステップ 8 フェールオーバー グループ 1 の管理 IP アドレスに接続して ASDM をプライマリ ユニットに接続し、セカンダリ ユニットで使用したのと同じファイルの場所を使用して、ASDM ソフトウェアをアップロードします。

ステップ 9 このイメージを ASDM イメージとして設定するように求められたら、[Yes] をクリックします。

ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。アップグレード ツールを終了します。**注**：ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM をリロードします。

ステップ 10 セカンダリ ユニットで使用したのと同じファイルの場所を使用して、ASA ソフトウェアをアップロードします。

ステップ 11 このイメージを ASA イメージとして設定するように求められたら、[Yes] をクリックします。

新しいイメージを使用するために、ASA をリロードするよう求められます。[OK] をクリックします。アップグレード ツールを終了します。

ステップ 12 コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。

これらの設定変更は、セカンダリ ユニットに自動的に保存されます。

ステップ 13 ASA FirePOWER モジュールをアップグレードする場合は、**[Tools]** > **[Command Line Interface]** を選択し、**no rest-api enable** を入力して ASA REST API を無効にします。

REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。

ステップ 14 **[Monitoring]** > **[Failover]** > **[Failover Group #]** の順に選択して、プライマリ ユニット上の両方のフェールオーバー グループをアクティブにします。ここで # は、プライマリ ユニットに移動するフェールオーバー グループの数です。[Make Active] をクリックします。

ステップ 15 セカンダリ ユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をフェールオーバー グループ 1 または 2 のスタンバイ管理 IP アドレスに接続します。アップグレードの完了を待ってから、ASDM をプライマリ ユニットに接続します。

ステップ 16 **[Monitoring]** > **[Failover]** > **[System]** の順に選択し、[Reload Standby] をクリックして、セカンダリユニットをリロードします。

[System] ペインを開いたまま、セカンダリユニットがリロードされるのを確認します。

ステップ 17 セカンダリ ユニットが起動したら、**[Monitoring]** > **[Failover]** > **[Failover Group #]** の順に選択して、セカンダリ ユニット上の両方のフェールオーバー グループをアクティブにします。ここで#は、セカンダリ ユニットに移動するフェールオーバー グループの数です。[Make Standby] をクリックします。

ASDM は、セカンダリ ユニット上のフェールオーバー グループ 1 の IP アドレスに自動的に再接続されます。

ステップ 18 プライマリ ユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をフェールオーバー グループ 1 または 2 のスタンバイ管理 IP アドレスに接続します。アップグレードの完了を待ってから、ASDM をセカンダリ ユニットに接続します。

ステップ 19 **[Monitoring]** > **[Failover]** > **[System]** の順に選択し、[Reload Standby] をクリックして、プライマリユニットをリロードします。

ステップ 20 フェールオーバーグループは、[Preempt Enabled] を使用して設定されると、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。ASDM は、プライマリ ユニット上のフェールオーバー グループ 1 の IP アドレスに自動的に再接続されます。

ASA クラスタのアップグレード

ASA クラスタをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、CLI または ASDM を使用します。

CLI を使用した ASA クラスタのアップグレード

ASA クラスタ内のすべての装置をアップグレードするには、次の手順を実行します。この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバ タイプについては、『ASA Command Reference』の **copy** コマンドを参照してください。

始める前に

- 制御ユニットで次の手順を実行します。ASA FirePOWER モジュールもアップグレードしている場合は、各データユニットへのコンソールアクセスまたは ASDM アクセスが必要です。クラスタ ユニットと状態（制御またはデータ）を表示するように ASA プロンプトを設定できます。これは、接続しているユニットを特定するのに役立ちます。prompt コマンドを参照してください。代わりに、**show cluster info** コマンドを入力して、各ユニットの役割を表示します。
- コンソール ポートを使用する必要があります。クラスタリングのイネーブルまたはディセーブルを、リモート CLI 接続から行うことはできません。

- マルチ コンテキスト モードでは、システム実行スペースで後続の手順を実行します。

手順

ステップ 1 特権 EXEC モード時に制御ユニットで、ASA ソフトウェアをクラスタ内のすべてのユニットにコピーします。

cluster exec copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

例：

```
asa/unit1/master# cluster exec copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin disk0:/asa9-15-1-smp-k8.bin
```

ステップ 2 ASDM イメージをクラスタ内のすべての装置にコピーします。

cluster exec copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

例：

```
asa/unit1/master# cluster exec copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asdm-77171417151.bin disk0:/asdm-77171417151.bin
```

ステップ 3 まだグローバル コンフィギュレーション モードを開始していない場合は、ここで開始します。

configure terminal

例：

```
asa/unit1/master# configure terminal
asa/unit1/master(config)#
```

ステップ 4 設定されている現在のブート イメージを表示します（最大 4 個）。

show running-config boot system

例：

```
asa/unit1/master(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。

ステップ 5 既存のブートイメージコンフィギュレーションがある場合は削除します。新しいブートイメージを最初の選択肢として入力できるようにするためです。

no boot system disk*n*:/[*path*/]*asa_image_name*

例：

```
asa/unit1/master(config)# no boot system disk0:/cdisk.bin
asa/unit1/master(config)# no boot system disk0:/asa931-smp-k8.bin
```

ステップ 6 ブートする ASA イメージを設定します（先ほどアップロードしたもの）。

boot system disk*n*:/[*path*/]*asa_image_name*

例：

```
asa/unit1/master(config)# boot system disk0://asa9-15-1-smp-k8.bin
```

このイメージが使用できない場合に使用するバックアップイメージに対して、このコマンドを繰り返します。たとえば、先ほど削除したイメージを再入力できます。

ステップ 7 使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

asdm image disk*n*:/[*path*/]*asdm_image_name*

例：

```
asa/unit1/master(config)# asdm image disk0:/asdm-77171417151.bin
```

使用するように設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

ステップ 8 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

これらの設定変更は、データユニットに自動的に保存されます。

ステップ 9 ASA FirePOWER モジュールをアップグレードする場合は、ASA REST API を無効にします。無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。

no rest-api agent

ステップ 10 ASDM で管理される ASA FirePOWER モジュールをアップグレードする場合は、ASDM を 個別の管理 IP アドレスに接続する必要があるため、ユニットごとに IP アドレスをメモする必要があります。

show running-config interface *management_interface_id*

使用されている **cluster-pool** プール名をメモします。

show ip[**v6**] **local pool** *poolname*

クラスタ ユニットの IP アドレスをメモしてください。

例：

```
asa/unit2/slave# show running-config interface gigabitethernet0/0
!
```

```
interface GigabitEthernet0/0
 management-only
 nameif inside
 security-level 100
 ip address 10.86.118.1 255.255.252.0 cluster-pool inside-pool
asa/unit2/slave# show ip local pool inside-pool
Begin           End             Mask            Free     Held     In use
10.86.118.16    10.86.118.17    255.255.252.0       0        0        2

Cluster Unit                    IP Address Allocated
unit2                           10.86.118.16
unit1                           10.86.118.17
asa1/unit2/slave#
```

ステップ 11 データユニットをアップグレードします。

ASA FirePOWER モジュールもアップグレードするかどうかによって、以下の手順を選択します。ASA FirePOWER 手順は、ASA FirePOWER モジュールもアップグレードした場合、ASA のリロードの回数が最小限に抑えられます。以下の手順では、データコンソールまたはASDM を使用するよう選択できます。すべてのコンソール ポートへのアクセスは準備できていないが、ASDM にネットワーク経由でアクセスできる場合は、コンソールではなく ASDM を使用することを推奨します。

（注） アップグレード プロセス中は、**cluster master unit** コマンドを使用して強制的にデータユニットを制御に変更しないでください。ネットワークの接続性とクラスタの安定性に関連した障害が発生する恐れがあります。最初にすべてのデータユニットをアップグレードしてリロードし、次にこの手順を実行すると、現在の制御ユニットから新しい制御ユニットへの移行をスムーズに行うことができます。

ASA FirePOWER モジュールをアップグレードしない場合：

a) 制御ユニットでメンバー名を表示するには、**cluster exec unit ?** または **show cluster info** コマンドを入力します。

b) データユニットをリロードします。

cluster exec unit *data-unit* **reload noconfirm**

例：

```
asa/unit1/master# cluster exec unit unit2 reload noconfirm
```

c) 各データユニットに対して手順を繰り返します。

接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち（約 5 分）、次の装置にこれらの手順を繰り返します。装置がクラスタに再接続したことを確認するには、**show cluster info** を入力します。

ASA FirePOWER モジュールもアップグレードする場合（データコンソールを使用）：

a) データユニットのコンソールポートに接続し、グローバル コンフィギュレーション モードに入ります。

enable

configure terminal

例：

```
asa/unit2/slave> enable
Password:
asa/unit2/slave# configure terminal
asa/unit2/slave(config)#
```

b) クラスタリングを無効にします。

cluster group *name*

no enable

リロード時にクラスタリングを有効にするために、この構成を保存しないでください。複数の障害を回避するにはクラスタリングを無効にして、アップグレードプロセスの間に再度参加させる必要があります。このユニットを再度参加させるのは、すべてのアップグレードとリロードが完了した場合のみです。

例：

```
asa/unit2/slave(config)# cluster group cluster1
asa/unit2/slave(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover
 either enable clustering or remove cluster group configuration.

Cluster unit unit2 transitioned from SLAVE to DISABLED
asa/unit2/ClusterDisabled(cfg-cluster)#
```

c) このデータユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、事前にメモした個別の管理 IP アドレスに ASDM を接続します。アップグレードが完了するまで待ちます。

d) データユニットをリロードします。

reload noconfirm

e) 各データユニットに対して手順を繰り返します。

接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち（約 5 分）、次の装置にこれらの手順を繰り返します。装置がクラスタに再接続したことを確認するには、**show cluster info** を入力します。

ASA FirePOWER モジュールもアップグレードする場合（ASDM を使用）：

a) 事前にメモしたこのデータユニットの「個別」の管理 IP アドレスに ASDM を接続します。
b) **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** の順に選択します。
c) [ASAクラスタに参加（Participate in ASA cluster）] チェックボックスをオフにします。

複数の障害を回避するにはクラスタリングを無効にして、アップグレードプロセスの間に再度参加させる必要があります。このユニットを再度参加させるのは、すべてのアップグレードとリロードが完了した場合のみです。

[Configure ASA cluster settings] チェックボックスをオフにしないでください。オフにすると、すべてのクラスタ コンフィギュレーションがクリアされ、ASDM が接続されている管理インターフェイスを含むすべてのインターフェイスもシャットダウンします。この場合、接続を復元するには、コンソール ポートで CLI にアクセスする必要があります。

（注） ASDM の以前のバージョンは、この画面でのクラスタの無効化をサポートしていません。この場合、**[Tools]** > **[Command Line Interface]** ツールを使用します。[Multiple Line] ラジオボタンをクリックして、**cluster group** *name* と **no enable** を入力します。クラスタ グループ名は、**[Home]** > **[Device Dashboard]** > **[Device Information]** > **[ASA Cluster]** エリアで確認できます。

d) [Apply] をクリックします。
e) ASDM から出るように促されます。同じ IP アドレスに ASDM を再接続します。
f) ASA FirePOWER モジュールをアップグレードします。

アップグレードが完了するまで待ちます。

g) ASDM で、**[Tools]** > **[System Reload]** を選択します。
h) [実行コンフィギュレーションを保存しないでリロードする（Reload without saving the running configuration）] オプション ボタンをクリックします。

この装置のリロード時にクラスタリングを有効にするために、この構成を保存しないようにします。

i) [Schedule Reload] をクリックします。
j) [Yes] をクリックしてリロードを続行します。
k) 各データユニットに対して手順を繰り返します。

接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち（約 5 分）、次の装置にこれらの手順を繰り返します。装置がクラスタに再接続したことを確認するには、制御ユニットの **[Monitoring]** > **[ASA Cluster]** > **[Cluster Summary]** ペインを確認します。

ステップ 12 制御ユニットをアップグレードします。

a) クラスタリングを無効にします。

cluster group *name*

no enable

新しい制御ユニットが選択され、トラフィックが安定するまで 5 分間待ちます。

リロード時にクラスタリングを有効にするために、この構成を保存しないでください。

可能であれば、制御ユニットのクラスタを手動で無効にすることを推奨します。これにより、新しい制御ユニットを迅速かつできるだけクリーンな状態で選定できます。

例：

```
asa/unit1/master(config)# cluster group cluster1
asa/unit1/master(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover
 either enable clustering or remove cluster group configuration.

Cluster unit unit1 transitioned from MASTER to DISABLED
asa/unit1/ClusterDisabled(cfg-cluster)#
```

b) このユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、事前にメモした個別の管理 IP アドレスに ASDM を接続します。この時点で、メインクラスタ IP アドレスは新しい制御ユニットに属しています。元の制御ユニットは、その個別の管理 IP アドレスに引き続きアクセスできます。

アップグレードが完了するまで待ちます。

c) このユニットをリロードします。

reload noconfirm

元の制御ユニットがクラスタに再接続すると、そのユニットはデータユニットになります。

ASDM を使用した ASA クラスタのアップグレード

ASA クラスタ内のすべての装置をアップグレードするには、次の手順を実行します。

始める前に

- 制御ユニットで次の手順を実行します。ASA FirePOWER モジュールもアップグレードしている場合は、各データユニットへの ASDM アクセスが必要です。
- マルチ コンテキスト モードでは、システム実行スペースで後続の手順を実行します。
- ローカル管理コンピュータに ASA と ASDM のイメージを配置します。

手順

ステップ 1 メインクラスタ IP アドレスに接続して、「制御」ユニットで ASDM を起動します。

この IP アドレスは、常に制御ユニットに保持されます。

ステップ 2 メイン ASDM アプリケーションウィンドウで、**[Tools]** > **[Upgrade Software from Local Computer]** の順に選択します。

[Upgrade Software from Local Computer] ダイアログボックスが表示されます。

ステップ 3 [クラスタ内のすべてのデバイス（All devices in the cluster）] オプション ボタンをクリックします。

[ソフトウェアのアップグレード（Upgrade Software）] ダイアログボックスが表示されます。

ステップ 4 [アップロードするイメージ（Image to Upload）] ドロップダウンリストから、[ASDM] を選択します。

ステップ 5 [ローカル ファイル パス（Local File Path）] フィールドで [ローカル ファイルの参照（Browse Local Files）] をクリックして、コンピュータ上のファイルを見つけます。

ステップ 6 （任意）[フラッシュファイルシステムのパス（Flash File System Path）] フィールドにフラッシュファイルシステムへのパスを入力するか、[フラッシュの参照（Browse Flash）] をクリックしてフラッシュファイルシステム上のディレクトリまたはファイルを検索します。

デフォルトでは、このフィールドにはパス（**disk0:/***filename*）が入力されています。

ステップ 7 [Upload Image] をクリックします。アップグレード プロセスには数分かかる場合があります。

ステップ 8 このイメージを ASDM イメージとして設定するように求められます。[Yes] をクリックします。

ステップ 9 ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。

アップグレード ツールを終了します。**注**：ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM をリロードします。

ステップ 10 これらの手順を繰り返し、[アップロードするイメージ（Image to Upload）] ドロップダウン リストから [ASA] を選択します。

ステップ 11 コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。

これらの設定変更は、データユニットに自動的に保存されます。

ステップ 12 **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Members]** で、各ユニットの個別の管理 IP アドレスをメモして、後で ASDM をデータユニットに直接接続できるようにします。

ステップ 13 ASA FirePOWER モジュールをアップグレードする場合は、**[ツール（Tools）]** > **[コマンドラインインターフェイス（Command Line Interface）]** を選択し、**no rest-api enable** を入力して ASA REST API を無効にします。

REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。

ステップ 14 データユニットをアップグレードします。

ASA FirePOWER モジュールもアップグレードするかどうかによって、以下の手順を選択します。ASA FirePOWER の手順では、ASA FirePOWER モジュールもアップグレードすると、ASA のリロードの回数が最も少なくなります。

（注） アップグレードプロセス中は、強制的にデータユニットを制御に変更するために **[Monitoring]** > **[ASA Cluster]** > **[Cluster Summary]** ページを使用して制御ユニットを変更しないでください。ネットワークの接続性とクラスタの安定性に関連した障害が発生する可能性があります。最初にすべてのデータユニットをリロードし、次にこの手順を実行すると、現在の制御ユニットから新しい制御ユニットへの移行をスムーズに行うことができます。

ASA FirePOWER モジュールをアップグレードしない場合：

a) 制御ユニットで、**[Tools]** > **[System Reload]** を選択します。
b) [Device] ドロップダウンリストからデータユニット名を選択します。
c) [Schedule Reload] をクリックします。
d) [Yes] をクリックしてリロードを続行します。
e) 各データユニットに対して手順を繰り返します。

接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち（約 5 分）、次の装置にこれらの手順を繰り返します。ユニットがクラスタに再接続したことを確認するには、**[Monitoring]** > **[ASA Cluster]** > **[Cluster Summary]** ペインを表示します。

ASA FirePOWER モジュールのアップグレードもある場合：

a) 制御ユニットで、**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Members]** を選択します。
b) アップグレードするデータユニットを選択して [Delete] をクリックします。
c) [適用（Apply）] をクリックします。
d) ASDM を終了し、事前にメモした「個別」の管理 IP アドレスに接続して、ASDM をデータユニットに接続します。
e) ASA FirePOWER モジュールをアップグレードします。

アップグレードが完了するまで待ちます。

f) ASDM で、**[Tools]** > **[System Reload]** を選択します。
g) [実行コンフィギュレーションを保存しないでリロードする（Reload without saving the running configuration）] オプション ボタンをクリックします。

この装置のリロード時にクラスタリングを有効にするために、この構成を保存しないようにします。

h) [Schedule Reload] をクリックします。
i) [Yes] をクリックしてリロードを続行します。
j) 各データユニットに対して手順を繰り返します。

接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち（約 5 分）、次の装置にこれらの手順を繰り返します。ユニットがクラスタに再接続したことを確認するには、**[Monitoring]** > **[ASA Cluster]** > **[Cluster Summary]** ペインを表示します。

ステップ 15 制御ユニットをアップグレードします。

a) 制御ユニットの ASDM で、**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** ペインを選択します。

b) [ASAクラスタに参加（Participate in ASA cluster）] チェックボックスをオフにして、[適用（Apply）] をクリックします。

ASDM から出るように促されます。

c) 新しい制御ユニットが選択され、トラフィックが安定するまで最大 5 分間待機します。

元の制御ユニットがクラスタに再接続すると、そのユニットはデータユニットになります。

d) 事前にメモした「個別」の管理 IP アドレスに接続して、ASDM を元の制御ユニットに再接続します。

この時点で、メインクラスタ IPアドレスは新しい制御ユニットに属しています。元の制御ユニットは、その個別の管理 IP アドレスに引き続きアクセスできます。

e) ASA FirePOWER モジュールをアップグレードします。

アップグレードが完了するまで待ちます。

f) **[Tools]** > **[System Reload]** を選択します。

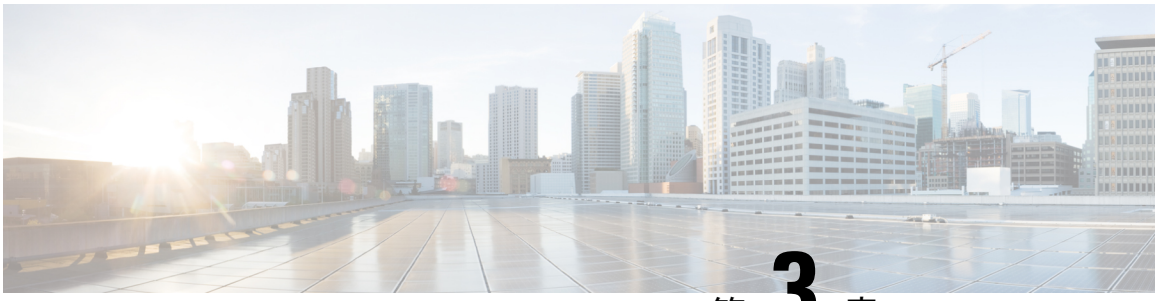
g) [実行コンフィギュレーションを保存しないでリロードする（Reload without saving the running configuration）] オプション ボタンをクリックします。

この装置のリロード時にクラスタリングを有効にするために、この構成を保存しないようにします。

h) [Schedule Reload] をクリックします。

i) [Yes] をクリックしてリロードを続行します。

ASDMから出るように促されます。メインクラスタ IPアドレスでASDMを再起動すると、新しい制御ユニットに再接続されます。



第 3 章

ASA FirePOWER モジュールのアップグレード

このドキュメントでは、管理方法の選択に応じて ASDM または Firepower Management Center を使用して ASA FirePOWER モジュールをアップグレードする方法について説明します。スタンドアロン、フェールオーバー、またはクラスタリングの各シナリオで FirePOWER アップグレードを実行するタイミングを判断するには、ASA アプライアンスまたは ASAv のアップグレード （85 ページ） を参照してください。

ASA FirePOWER アップグレード時の動作

ASA FirePOWER module にトラフィックをリダイレクトする ASA サービス ポリシーは、Firepower ソフトウェア アップグレードの間（Snort プロセスを再起動する特定の設定を導入するときなど）にモジュールがトラフィックを処理する方法を決定します。

表 *15 : ASA FirePOWER* アップグレード中のトラフィックの動作

トラフィック リダイレクションのポリシー	トラフィックの動作
フェール オープン（**sfr fail-open**）	インスペクションなしで転送
フェール クローズ（**sfr fail-close**）	ドロップされる
モニタのみ（**sfr {fail-close}|{fail-open} monitor-only**）	パケットをただちに出力、コピーへのインスペクションなし

ASA FirePOWER 展開時のトラフィックの動作

Snort プロセスを再起動している間のトラフィックの動作は、ASA FirePOWER module をアップグレードする場合と同じです。

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『『Firepower Management Center 構成ガイド』』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、Snort プロセスを再起動すると、トラフィック インスペクションが中断されます。サービスポリシーにより、中断中にインスペクションせずにトラフィックをドロップするか通過するかが決定されます。

ASDM によって管理される ASA FirePOWER モジュールのアップグレード

次の手順を使用して、ASDM によって管理される ASA FirePOWER モジュールをアップグレードします。

⚠

注意 構成の変更、手動による再起動、またはアップグレードモジュールのシャットダウンは行わないでください。進行中のアップグレードは再開しないでください。事前のチェック中に、アップグレード プロセスが停止しているように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

手順

ステップ 1 ASA のサポートされるバージョンを実行していることを確認します。

ASA と ASA FirePOWER のバージョンには広く互換性があります。ただし、厳密には ASA のアップグレードが必要でない場合でも、問題解決のために、サポートされた最新のバージョンへのアップグレードが必要になることがあります。

そのシーケンスで ASA FirePOWER モジュールをアップグレードする場合の、スタンドアロン、フェールオーバー、クラスタリングのシナリオにおける ASA のアップグレード手順を参照してください。ASA ソフトウェアをアップグレードしない場合でも、ASA のフェールオーバーとクラスタリング アップグレード手順を参照する必要があります。これにより、モジュールのアップグレード前に装置でフェールオーバーまたはクラスタリングの無効化を実行して、トラフィックの損失を回避できます。たとえば、クラスタでは、各セカンダリ ユニットを順次

アップグレードし（クラスタリングの無効化、モジュールのアップグレード、クラスタリングの再有効化を含む）、その後プライマリ ユニットをアップグレードする必要があります。

ステップ 2 アップグレード パッケージは Cisco.com からダウンロードします。

メジャー バージョンの場合。

- バージョン 6.0 ～ 6.2.2 へのアップグレード：
  Cisco_Network_Sensor_**Upgrade**-[version]-[build].**sh**
- バージョン 6.2.3 以降へのアップグレード：
  Cisco_Network_Sensor_**Upgrade**-[version]-[build].**sh.REL.tar**

パッチの場合。

- 5.4.1.x ～ 6.2.1.x へのアップグレード：Cisco_Network_Sensor_**Patch**-[version]-[build].**sh**
- バージョン 6.2.2.1 以降へのアップグレード：
  Cisco_Network_Sensor_**Patch**-[version]-[build].**sh.REL.tar**

シスコサポートおよびダウンロードサイトから直接ダウンロードします。電子メールでパッケージを転送すると、破損する可能性があります。バージョン 6.2.2+ 以降のアップグレード パッケージは署名付きで、単純な .sh ではなく .sh.REL.tar の末尾になります。署名付きのアップグレード パッケージは解凍しないでください。

ステップ 3 ASDM を使用して ASA に接続し、アップグレード パッケージをアップロードします。

a) **[構成（Configuration）] > [ASA FirePOWER の構成（ASA FirePOWER Configuration）] > [Updates]**を選択します。
b) [更新のアップロード（Upload Update）] をクリックします。
c) [ファイルの選択（Choose File）] をクリックして対象ファイルに移動し、更新を選択します。
d) [Upload] をクリックします。

ステップ 4 保留中の構成の変更を展開します。展開しない場合、アップグレードが失敗することがあります。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。詳細については、ASA FirePOWER アップグレード時の動作 （145 ページ） を参照してください。

ステップ 5 （バージョン 6.1 以降へのアップグレード）ASA REST API を無効にします。

REST API を無効にしない場合、アップグレードは失敗します。ASA FirePOWER モジュールのバージョン 6.0 以降も実行している場合、ASA 5506-X シリーズのデバイスでは ASA REST API はサポートされません。

ASA の CLI を使用して、REST API を無効にします。

no rest-api agent

次のコマンドを実行して、アップグレード後に REST API を再度有効にすることができます。

rest-api agent

ステップ 6 **[モニタリング（Monitoring）] > [ASA FirePOWER のモニタリング（ASA FirePOWER Monitoring）] > [タスク ステータス（Task Status）]** の順に選択して、必須タスクが完了していることを確認します。

アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。後で失敗ステータス メッセージを手動で削除できます。

ステップ 7 **[構成（Configuration）] > [ASA FirePOWER の構成（ASA FirePOWER Configuration）] > [Updates]**を選択します。

ステップ 8 アップロードしたアップグレード パッケージの横にある [インストール（Install）] アイコンをクリックして、モジュールをアップグレードして再起動することを確認します。

トラフィックは、モジュールの設定方法に応じて、アップグレード中にドロップされるか、または検査されることなくネットワークを通過します。詳細については、ASA FirePOWER アップグレード時の動作 （145 ページ）を参照してください。

ステップ 9 [タスク ステータス（Task Status）] ページでアップグレードの進行状況をモニタします。

モジュールのアップグレード中は、そのモジュールに構成の変更を加えないでください。アップグレード ステータスに進行状況が数分間表示されない、またはアップグレードが失敗したことが示されている場合でも、アップグレードを再開したり、デバイスを再起動したりしないでください。代わりに、Cisco TAC に連絡してください。

ステップ 10 アップグレードが完了したら、ASDM を ASA に再接続します。

ステップ 11 **[構成（Configuration）] > [ASA FirePOWER の構成（ASA FirePOWER Configuration）]** の順に選択して、[更新（Refresh）] をクリックします。そうしない場合、インターフェイスが予期しない動作を示すことがあります。

ステップ 12 **[構成（Configuration）] > [ASA FirePOWER の構成（ASA FirePOWER Configuration）] > [システム情報（System Information）]** の順に選択して、モジュールのソフトウェア バージョンが正しいことを確認します。

ステップ 13 サポート サイトで利用可能な侵入ルールの更新や脆弱性データベース（VDB）が現在実行中のバージョンより新しい場合は、新しいバージョンをインストールします。

ステップ 14 リリース ノートに記載されているアップグレード後の構成の変更をすべて完了します。

ステップ 15 構成を再展開します。

Firepower Management Center のアップグレード

Firepower Management Center を使用して ASA FirePOWER モジュールを管理している場合は、モジュールをアップグレードする前に Management Center をアップグレードする必要があります。

スタンドアロンの FMC のアップグレード

この手順を使用して、Firepower Management Center Virtual などのスタンドアロン Firepower Management Center をアップグレードします。

⚠

注意 アップグレードしているアプライアンスとの間での変更の展開、またはアップグレードしているアプライアンスの手動での再起動やシャットダウンは行わないでください。進行中のアップグレードを再開しないでください。事前のチェック中に、アップグレードプロセスが停止しているように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

始める前に

ホスト環境と管理対象デバイス アップグレードを含む、アップグレード パスでの位置を確認します。この手順を完全に計画して準備していることを確認します。

手順

ステップ 1 構成が古い管理対象デバイスに展開します。

メニューバーで、[展開（Deploy）]をクリックします。FMCデバイスを選択し、[展開（Deploy）]をもう一度クリックします。アップグレードする前に展開すると、失敗する可能性が減少します。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。

ステップ 2 アップグレード前の最終的なチェックを実行します。

- 正常性のチェック：メッセージ センターを使用します（メニュー バーの [System Status] アイコンをクリックします）。導入環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。
- タスクの実行：また、メッセージセンターで、必須タスクが完了していることを確認します。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。後で失敗ステータス メッセージを手動で削除できます。
- ディスク容量のチェック：最終的なディスク容量のチェックを実行します。空きディスク容量が十分でない場合、アップグレードは失敗します。

ステップ 3 **[System]** > **[Updates]** を選択します。

ステップ 4 使用するアップグレードパッケージの横にある [インストール（Install）] アイコンをクリックして、FMC を選択します。

ステップ 5 [Install] をクリックすると、アップグレードが開始されます。

アップグレードして、FMC を再起動することを確認します。

ステップ 6 ログアウトするまで、メッセージ センターで事前チェックの進行状況をモニタします。

FMC のアップグレード中は、構成に変更を加えたり、デバイスに構成を展開したりしないでください。メッセージセンターに進行状況が数分間表示されない、またはアップグレードが失敗したことが示されている場合でも、アップグレードを再開したり、FMC を再起動したりしないでください。代わりに、Cisco TAC にお問い合わせください。

ステップ 7 可能なときに、FMC に再度ログインします。

- マイナーアップグレード（パッチとホットフィックス）：アップグレードが完了し、FMC が再起動した後にログインできます。
- メジャー アップグレード：アップグレードが完了する前にログインできます。アップグレードの進行状況をモニタし、アップグレード ログとエラー メッセージを確認するために使用できるページが FMC に表示されます。アップグレードが完了し、FMC が再起動すると再度ログアウトされます。リブート後に、再ログインしてください。

ステップ 8 プロンプトが表示されたら、エンド ユーザ ライセンス契約書（EULA）を確認し、承認します。

ステップ 9 アップグレードが成功したことを確認します。

ログイン時に、FMC からアップグレードの成功メッセージが表示されない場合は、**[ヘルプ（Help）]** > **[バージョン情報（About）]** を選択して、現在のソフトウェアのバージョン情報を表示します。

ステップ 10 メッセージ センターを使用して、導入環境に問題がないことを再度確認します。

ステップ 11 侵入ルール（SRU）および脆弱性データベース（VDB）を更新します。

シスコ サポート & ダウンロード サイトで利用可能な SRU や VDB が現在実行中のバージョンより新しい場合は、新しいバージョンをインストールします。詳細については、『Firepower Management Center 構成ガイド』を参照してください。侵入ルールを更新する場合、ポリシーを自動的に再適用する必要はありません。後で適用します。

ステップ 12 リリース ノートに記載されているアップグレード後の構成の変更をすべて完了します。

ステップ 13 構成を再展開します。

すべての管理対象デバイスに再展開します。デバイスに構成を展開しない場合、最終的なアップグレードが失敗し、イメージの再作成が必要になることがあります。

ハイ アベイラビリティ FMC のアップグレード

この手順を使用して、ハイ アベイラビリティ ペアに含まれる Firepower Management Center の Firepower ソフトウェアをアップグレードします。

一度に 1 つのピアをアップグレードします。同期を一時停止した状態で、最初にスタンバイをアップグレードし、次にアクティブをアップグレードします。スタンバイ FMC で事前チェックが開始されると、ステータスがスタンバイからアクティブに切り替わり、両方のピアがアクティブになります。この一時的な状態は *split-brain* と呼ばれていて、アップグレード中を除き、サポートされていません。ペアが split-brain の状況で、構成の変更または展開を行わないでください。同期の再開後は変更内容が失われます。

⚠

注意 アップグレードしているアプライアンスとの間での変更の展開、またはアップグレードしているアプライアンスの手動での再起動やシャットダウンは行わないでください。進行中のアップグレードを再開しないでください。事前のチェック中に、アップグレードプロセスが停止しているように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

始める前に

管理対象デバイスのアップグレードなどに関するアップグレードパス内の場所を確認します。この手順を完全に計画して準備していることを確認します。

手順

ステップ 1 アクティブな FMC で、構成が古い管理対象デバイスに展開します。

メニューバーで、[展開（Deploy）]をクリックします。FMCデバイスを選択し、[展開（Deploy）]をもう一度クリックします。アップグレードする前に展開すると、失敗する可能性が減少します。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。

ステップ 2 同期を一時停止する前に、メッセージセンターを使用して導入環境に問題がないことを確認します。

FMC メニューバーで、[システム ステータス（System Status）]アイコンをクリックして、メッセージセンターを表示します。導入環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。

ステップ 3 同期を一時停止します。

a) **[システム（System）]** > **[統合（[Integration）]**を選択します。

b) [ハイ アベイラビリティ（High Availability）] タブで、[同期の一時停止（Pause Synchronization）] をクリックします。

ステップ 4 FMC を一度に 1 つずつアップグレード： 最初はスタンバイ、次はアクティブです。

「スタンドアロンの FMC のアップグレード （149 ページ）」の手順に従います。ただし、初期の展開は省略し、各 FMC で更新が成功したことを確認したら停止します。要約すると、それぞれの FMC で以下の手順を実行します。

a) 最終的なアップグレード前チェック（健全性、実行中のタスク、ディスク容量）を実行します。
b) [System][Updates] > ページで、アップグレードをインストールします。
c) ログアウトするまで進行状況をモニタし、可能な場合な再度ログインします（これは主なアップグレードで 2 回行われます）。
d) アップグレードが成功したことを確認します。

ペアが split-brain の状況で、構成の変更または展開を行わないでください。

ステップ 5 アクティブ ピアにする FMC で、同期を再開します。

a) **[システム（System）] > [統合（Integration）]** の順に選択します。
b) [ハイ アベイラビリティ（High Availability）] タブで、[アクティブにする（Make-Me-Active）] をクリックします。
c) 同期が再開し、その他の FMC がスタンバイ モードに切り替わるまで待ちます。

ステップ 6 メッセージ センターを使用して、導入環境に問題がないことを再度確認します。

ステップ 7 侵入ルール（SRU）および脆弱性データベース（VDB）を更新します。

シスコ サポート & ダウンロード サイトで利用可能な SRU や VDB が現在実行中のバージョンより新しい場合は、新しいバージョンをインストールします。詳細については、『Firepower Management Center 構成ガイド』を参照してください。侵入ルールを更新する場合、ポリシーを自動的に再適用する必要はありません。後で適用します。

ステップ 8 リリース ノートに記載されているアップグレード後の構成の変更をすべて完了します。

ステップ 9 構成を再展開します。

すべての管理対象デバイスに再展開します。デバイスに構成を展開しない場合、最終的なアップグレードが失敗し、イメージの再作成が必要になることがあります。

FMCによって管理されるASAFirePOWERモジュールのアップグレード

この手順を使用して、FMC によって管理される ASA FirePOWER module をアップグレードします。モジュールをいつアップグレードするかは、ASAをアップグレードするかどうか、およびASAの展開によって異なります。

- スタンドアロン ASA デバイスをアップグレードする場合：ASA もアップグレードする場合は、ASA をアップグレードしてリロードした直後に、FMC を使用して ASA FirePOWER モジュールをアップグレードします。
- ASA クラスタとフェールオーバ ペアをアップグレードする場合：トラフィック フローとインスペクションの中断を避けるには、これらのデバイスを 1 つずつ完全にアップグレードします。ASA をアップグレードする場合、各ユニットをリロードして ASA をアップグレードする直前に、FMC を使用して ASA FirePOWER モジュールをアップグレードします。

詳細については、「Asa FirePOWER アップグレードパス：FMC 搭載アップグレードパス：ASA FirePOWER （44 ページ）」と ASA アップグレード手順を参照してください。

注意 アップグレードしているアプライアンスとの間での変更の展開、またはアップグレードしているアプライアンスの手動での再起動やシャットダウンは行わないでください。進行中のアップグレードを再開しないでください。事前のチェック中に、アップグレードプロセスが停止しているように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

始める前に

ASA や FMC のアップグレードなどに関するアップグレード パス内の場所を確認します。この手順を完全に計画して準備していることを確認します。

手順

ステップ 1 アップグレード対象デバイスに構成を展開します。

メニューバーで、[展開（Deploy）]をクリックします。FMCデバイスを選択し、[展開（Deploy）]をもう一度クリックします。アップグレードする前に展開すると、失敗する可能性が減少します。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。詳細については、ASA FirePOWER アップグレード時の動作 （145 ページ） を参照してください。

ステップ 2 （バージョン 6.1 以降へのアップグレード）ASA REST API を無効にします。

REST API を無効にしない場合、アップグレードは失敗します。ASA FirePOWER モジュールのバージョン 6.0 以降も実行している場合、ASA 5506-X シリーズのデバイスでは ASA REST API はサポートされません。

ASA の CLI を使用して、REST API を無効にします。

no rest-api agent

次のコマンドを実行して、アップグレード後に REST API を再度有効にすることができます。

rest-api agent

ステップ 3 アップグレード前の最終的なチェックを実行します。

- 正常性のチェック：メッセージ センターを使用します（メニュー バーの [System Status] アイコンをクリックします）。導入環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。
- タスクの実行：また、メッセージセンターで、必須タスクが完了していることを確認します。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。後で失敗ステータス メッセージを手動で削除できます。
- ディスク容量のチェック：最終的なディスク容量のチェックを実行します。空きディスク容量が十分でない場合、アップグレードは失敗します。

ステップ 4 **[System]** > **[Updates]** を選択します。

ステップ 5 使用するアップグレード パッケージの横にある [インストール（Install）] アイコンをクリックして、アップグレードするデバイスを選択します。

アップグレードするデバイスがリストに表示されない場合は、間違ったアップグレード パッケージを選択しています。

（注） 同時にアップグレードするデバイスは 5 台までにすることを強く推奨します。FMC では選択したすべてのデバイスがそのプロセスを完了するまで、アップグレードを停止することはできません。いずれかのデバイスのアップグレードに問題がある場合、問題を解決する前に、すべてのデバイスのアップグレードを完了する必要があります。

ステップ 6 [Install] をクリックし、アップグレードして、デバイスを再起動することを確認します。

トラフィックは、デバイスの設定および展開方法に応じて、アップグレードの間ドロップするか、検査なしでネットワークを通過します。詳細については、ASA FirePOWER アップグレード時の動作 （145 ページ） を参照してください。

ステップ 7 メッセージ センターでアップグレードの進行状況をモニタします。

デバイスのアップグレード中は、構成をそのデバイスに展開しないでください。メッセージセンターに進行状況が数分間表示されない、またはアップグレードが失敗したことが示されている場合でも、アップグレードを再開したり、デバイスを再起動したりしないでください。代わりに、Cisco TAC にお問い合わせください。

ステップ 8 成功したことを確認します。

アップグレードが完了したら、**[デバイス（Devices）]**>**[デバイス管理（Device Management）]** を選択し、アップグレードしたデバイスのソフトウェア バージョンが正しいことを確認します。

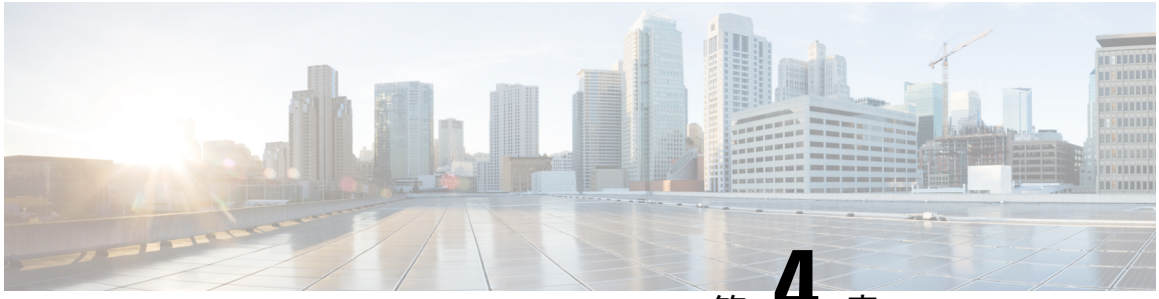
ステップ 9 メッセージ センターを使用して、導入環境に問題がないことを再度確認します。

ステップ 10 侵入ルール（SRU）および脆弱性データベース（VDB）を更新します。

シスコ サポート & ダウンロード サイトで利用可能な SRU や VDB が現在実行中のバージョンより新しい場合は、新しいバージョンをインストールします。詳細については、『Firepower Management Center 構成ガイド』を参照してください。侵入ルールを更新する場合、ポリシーを自動的に再適用する必要はありません。後で適用します。

ステップ 11 リリース ノートに記載されているアップグレード後の構成の変更をすべて完了します。

ステップ 12 アップグレードしたデバイスに構成を再度展開します。



第 4 章

FirePOWER 4100/9300 の ASA をアップグレード

このドキュメントでは、Firepower 4100/9300 で ASA をアップグレードする方法について説明します。

FXOS および ASA スタンドアロン デバイスまたはシャーシ内クラスタのアップグレード

FXOS CLI または Firepower Chassis Manager を使用して、Firepower 9300 上のFXOS およびスタンドアロン ASA デバイスまたは ASA シャーシ内クラスタをアップグレードします。

以下を使用したFXOSおよびASAスタンドアロンデバイスまたはシャーシ内クラスタのアップグレード Firepower Chassis Manager

アップグレード プロセスは最大 45 分かかることがあります。アップグレード中、トラフィックはデバイスを通過しません。適切なアップグレード活動の計画を行ってください。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS および ASA ソフトウェア パッケージをダウンロードします（Cisco.com からのソフトウェアのダウンロード （51 ページ）を参照してください）。
- FXOS と ASA の構成をバックアップします。

手順

ステップ 1 Firepower Chassis Manager で、**[System]** > **[Updates]** を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。

ステップ 2 新しい FXOS プラットフォーム バンドルのイメージと ASA ソフトウェア イメージのアップロード：：

（注） FXOS 2.3.1 より前のバージョンにアップグレードする場合、FXOS プラットフォーム バンドル ソフトウェアをアップグレードするまでは、ASA CSP イメージをセキュリティ アプライアンスにアップロードしないでください。

a) [Upload Image] をクリックします。
b) [Choose File] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。
c) [Upload] をクリックします。
選択したイメージがシャーシにアップロードされます。

ステップ 3 新しい FXOS プラットフォーム バンドル イメージが正常にアップロードされたら、アップグレードする FXOS プラットフォーム バンドルの [Upgrade] をクリックします。

システムは、まずインストールするソフトウェア パッケージを確認します。現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

ステップ 4 [はい（Yes）] をクリックして、インストールを続行することを確認します。

FXOS がバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 5 Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレードプロセスをモニタできます（アップグレード進行のモニタ （197 ページ） を参照してください）。

ステップ 6 すべてのコンポーネントが正常にアップグレードされたら、続行する前に、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します（インストールの確認 （198 ページ） を参照してください）。

ステップ 7 [論理デバイス（Logical Devices）] を選択します。
[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。

ステップ 8 アップグレードする各 ASA 論理デバイスごとに、以下を実行います。

a) 更新する論理デバイスの [Set Version] アイコンをクリックして、[Update Image Version] ダイアログボックスを開きます。

b) [New Version] では、アップグレードしたいソフトウェア バージョンを選択します。
c) [OK] をクリックします。

ステップ 9 アップグレードプロセスが完了したら、アプリケーションがオンラインであり、正常にアップグレードされたことを確認します。

a) [論理デバイス（Logical Devices）] を選択します。
b) アプリケーションのバージョンと動作ステータスを確認します。

FXOS CLI を使用した FXOS および ASA スタンドアロン デバイスまたはシャーシ内クラスタのアップグレード

アップグレード プロセスは最大 45 分かかることがあります。アップグレード中、トラフィックはデバイスを通過しません。適切なアップグレード活動の計画を行ってください。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS および ASA ソフトウェア パッケージをダウンロードします（Cisco.com からのソフトウェアのダウンロード （51 ページ）を参照してください）。
- FXOS と ASA の構成をバックアップします。
- シャーシにソフトウェア イメージをダウンロードするために必要な次の情報を収集します。
  - イメージのコピー元のサーバの IP アドレスおよび認証クレデンシャル。
  - イメージ ファイルの完全修飾名。

手順

ステップ 1 FXOS CLI に接続します。

ステップ 2 新しいプラットフォーム バンドル イメージをシャーシにダウンロードします。

a) ファームウェア モードを開始します。

scope firmware

b) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

download image *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@server*/*path*/*image_name*
- **scp**://*username@server*/*path*/*image_name*

- **sftp**://*username@server*/*path*/*image_name*
- **tftp**://*server*:*port-num*/*path*/*image_name*

c) ダウンロード プロセスをモニタする場合：

scope download-task *image_name*

show detail

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

ステップ 3 新しいFXOSプラットフォーム バンドルのイメージが正常にダウンロードされたら、FXOSバンドルをアップグレードします。

a) 必要に応じて、ファームウェア モードに戻ります。

up

b) インストールする FXOS プラットフォーム バンドルのバージョン番号をメモします。

show package

c) auto-install モードにします。

scope auto-install

d) FXOS プラットフォーム バンドルをインストールします。

install platform platform-vers *version_number*

version_number は、インストールする FXOS プラットフォーム バンドルのバージョン番号です（たとえば、2.3(1.58)）。

e) システムは、まずインストールするソフトウェア パッケージを確認します。現在インストールされているアプリケーションと指定したFXOSプラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

yes を入力して、検証に進むことを確認します。

f) インストールの続行を確定するには**yes** を、インストールをキャンセルするには**no** を入力します。

FXOS がバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

g) アップグレードプロセスをモニタするには、アップグレード進行のモニタ （197 ページ）を参照してください。

ステップ 4 すべてのコンポーネントが正常にアップグレードされたら、続行する前に、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します（インストールの確認 （198 ページ） を参照してください）。

ステップ 5 シャーシに新しい ASA ソフトウェア イメージをダウンロードします。

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) アプリケーション ソフトウェア モードを開始します。

scope app-software

c) 論理デバイス ソフトウェア イメージをダウンロードします。

download image *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@server*/*path*
- **scp**://*username@server*/*path*
- **sftp**://*username@server*/*path*
- **tftp**://*server*:*port-num*/*path*

d) ダウンロード プロセスをモニタする場合：

show download-task

e) ダウンロードしたアプリケーションを表示する場合：

up

show app

ダウンロードしたソフトウェアパッケージの ASA のバージョンをメモします。後の手順でアプリケーションを有効にするために、正確なバージョン文字列を使用する必要があります。

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
```

```
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State

    ---------------------------- ---------- -------------------- --------------- -----

    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1          user
Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

ステップ 6 アップグレードする各 ASA 論理デバイスごとに、以下を実行います。

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) スコープを更新するセキュリティ モジュールに設定します。

scope slot*slot_number*

c) スコープを更新する ASA アプリケーションに設定します。

FXOS 2.3.1 以前： **scope app-instance asa**

FXOS 2.4.1 以降：**scope app-instance asa** *instance_name*

d) スタートアップ バージョンを新しい ASA ソフトウェアのバージョンに設定します。

set startup-version *version_number*

ステップ 7 設定をコミットします。

commit-buffer

トランザクションをシステムの設定にコミットします。アプリケーション イメージが更新され、アプリケーションが再起動します。

ステップ 8 セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認するには、インストールの確認 （198 ページ） を参照してください。

FXOS および ASA アクティブ/スタンバイ フェールオーバー ペアのアップグレード

FXOS CLI または Firepower Chassis Manager を使用して、FXOS および ASA アクティブ/スタンバイ フェールオーバー ペアをアップグレードします。

Firepower Chassis Manager を使用した FXOS および ASA アクティブ/スタンバイ フェールオーバー ペアのアップグレード

アップグレード プロセスはシャーシごとに最大 45 分かかることがあります。適切なアップグレード活動の計画を行ってください。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アクティブになっているユニットとスタンバイになっているユニットを確認する必要があります。ASDM をアクティブな ASA の IP アドレスに接続します。アクティブ装置は、常にアクティブな IP アドレスを保有しています。次に、**[モニタリング（Monitoring）]** > **[プロパティ（Properties）]** > **[フェールオーバー（Failover）]** > **[ステータス（Status）]** の順に選択して、このユニットの優先順位（プライマリまたはセカンダリ）を表示し、接続先のユニットを確認できるようにします。
- アップグレード先の FXOS および ASA ソフトウェア パッケージをダウンロードします（Cisco.com からのソフトウェアのダウンロード （51 ページ）を参照してください）。
- FXOS と ASA の構成をバックアップします。

手順

ステップ 1 スタンバイ ASA 論理デバイスが含まれている Firepower セキュリティ アプライアンスでは、新しい FXOS プラットフォーム バンドル イメージと ASA ソフトウェア イメージをアップロードします：

（注） FXOS 2.3.1 より前のバージョンにアップグレードする場合、FXOS プラットフォーム バンドル ソフトウェアをアップグレードするまでは、ASA CSP イメージをセキュリティ アプライアンスにアップロードしないでください。

a) Firepower Chassis Manager で、**[システム（System）]** > **[更新（Updates）]** を選択します。[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。
b) [Upload Image] をクリックします。
c) [Choose File] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。

d) [Upload] をクリックします。
選択したイメージがシャーシにアップロードされます。

ステップ 2 新しい FXOS プラットフォーム バンドル イメージが正常にアップロードされた後に、スタンバイ ASA 論理デバイスが含まれている Firepower セキュリティ アプライアンスの FXOS バンドルをアップグレードします。

a) アップグレードする FXOS プラットフォーム バンドルの [Upgrade] アイコンをクリックします。

システムは、まずインストールするソフトウェア パッケージを確認します。現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

b) [はい（Yes）] をクリックして、インストールを続行することを確認します。

FXOS がバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 3 Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレードプロセスをモニタできます（アップグレード進行のモニタ （197 ページ） を参照してください）。

ステップ 4 すべてのコンポーネントが正常にアップグレードされたら、続行する前に、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します（インストールの確認 （198 ページ） を参照してください）。

ステップ 5 ASA 論理デバイス イメージのアップグレード：

a) [Logical Devices] を選択して [Logical Devices] ページを開きます。
[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。

b) 更新する論理デバイスの [Set Version] アイコンをクリックして、[Update Image Version] ダイアログボックスを開きます。

c) [New Version] では、更新後のソフトウェア バージョンを選択します。

d) [OK] をクリックします。

ステップ 6 アップグレードプロセスが完了したら、アプリケーションがオンラインであり、正常にアップグレードされたことを確認します。

a) [論理デバイス（Logical Devices）] を選択します。

b) アプリケーションのバージョンと動作ステータスを確認します。

ステップ 7 アップグレードしたユニットをアクティブユニットにして、アップグレード済みのユニットにトラフィックが流れるようにします。

a) スタンバイ ASA IP アドレスに接続して、スタンバイ装置で ASDM を起動します。

b) **[モニタリング（Monitoring）] > [プロパティ（Properties）] > [フェールオーバー（Failover）] > [ステータス（Status）]** の順に選択し、[アクティブにする（Make Active）] をクリックして、スタンバイ装置を強制的にアクティブにします。

ステップ 8 新しいスタンバイ ASA 論理デバイスが含まれている Firepower セキュリティ アプライアンスでは、新しい FXOS プラットフォーム バンドル イメージと ASA ソフトウェア イメージをアップロードします：

（注） FXOS 2.3.1 より前のバージョンにアップグレードする場合、FXOS プラットフォーム バンドル ソフトウェアをアップグレードするまでは、ASA CSP イメージをセキュリティ アプライアンスにアップロードしないでください。

a) Firepower Chassis Manager で、**[システム（System）] > [更新（Updates）]** を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。
b) [Upload Image] をクリックします。
c) [Choose File] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。
d) [Upload] をクリックします。
選択したイメージがシャーシにアップロードされます。

ステップ 9 新しい FXOS プラットフォーム バンドル イメージが正常にアップロードされた後に、新しいスタンバイ ASA 論理デバイスが含まれている Firepower セキュリティ アプライアンスの FXOS バンドルをアップグレードします。

a) アップグレードする FXOS プラットフォーム バンドルの [Upgrade] アイコンをクリックします。

システムは、まずインストールするソフトウェア パッケージを確認します。現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

b) [はい（Yes）] をクリックして、インストールを続行することを確認します。

FXOS がバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 10 Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレード プロセスをモニタできます（アップグレード進行のモニタ （197 ページ） を参照してください）。

ステップ 11 すべてのコンポーネントが正常にアップグレードされたら、続行する前に、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します（インストールの確認 （198 ページ） を参照してください）。

ステップ 12 ASA 論理デバイス イメージのアップグレード：

a) [論理デバイス（Logical Devices）] を選択します。
[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。論理デバイスが設定されていない場合は、これを通知するメッセージが代わりに表示されます。
b) 更新する論理デバイスの [Set Version] アイコンをクリックして、[Update Image Version] ダイアログボックスを開きます。
c) [New Version] では、更新後のソフトウェア バージョンを選択します。

d) [OK] をクリックします。

ステップ 13 アップグレードプロセスが完了したら、アプリケーションがオンラインであり、正常にアップグレードされたことを確認します。

a) [論理デバイス（Logical Devices）] を選択します。
b) アプリケーションのバージョンと動作ステータスを確認します。

ステップ 14 （オプション）アップグレードしたユニットを、アップグレード前のようにアクティブユニットにします。

a) スタンバイ ASA IP アドレスに接続して、スタンバイ装置で ASDM を起動します。
b) **[モニタリング（Monitoring）] > [プロパティ（Properties）] > [フェールオーバー（Failover）] > [ステータス（Status）]** の順に選択し、[アクティブにする（Make Active）] をクリックして、スタンバイ装置を強制的にアクティブにします。

FXOS CLI を使用した FXOS および ASA アクティブ/スタンバイ フェールオーバー ペアのアップグレード

アップグレード プロセスはシャーシごとに最大 45 分かかることがあります。適切なアップグレード活動の計画を行ってください。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- どのユニットがアクティブでどのユニットがスタンバイかを特定する必要があります。Firepower セキュリティ アプライアンスで ASA コンソールに接続し、**show failover** コマンドを入力してユニットのアクティブ/スタンバイ状態を表示します。
- アップグレード先の FXOS および ASA ソフトウェア パッケージをダウンロードします（Cisco.com からのソフトウェアのダウンロード （51 ページ）を参照してください）。
- FXOS と ASA の構成をバックアップします。
- シャーシにソフトウェア イメージをダウンロードするために必要な次の情報を収集します。
  - イメージのコピー元のサーバの IP アドレスおよび認証クレデンシャル。
  - イメージ ファイルの完全修飾名。

手順

ステップ 1 スタンバイ ASA 論理デバイスが含まれている Firepower セキュリティ アプライアンスでは、新しい FXOS プラットフォーム バンドル イメージとをアップロードします：

a) FXOS CLI に接続します。
b) ファームウェア モードを開始します。

scope firmware

c) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

download image *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@server*/*path*/*image_name*
- **scp**://*username@server*/*path*/*image_name*
- **sftp**://*username@server*/*path*/*image_name*
- **tftp**://*server*:*port-num*/*path*/*image_name*

d) ダウンロード プロセスをモニタする場合：

scope download-task *image_name*

show detail

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

ステップ 2 新しいFXOSプラットフォーム バンドルのイメージが正常にダウンロードされたら、FXOS バンドルをアップグレードします。

a) 必要に応じて、ファームウェア モードに戻ります。

up

b) インストールする FXOS プラットフォーム バンドルのバージョン番号をメモします。

show package

c) auto-install モードにします。

scope auto-install

d) FXOS プラットフォーム バンドルをインストールします。

install platform platform-vers *version_number*

version_number は、インストールする FXOS プラットフォーム バンドルのバージョン番号です（たとえば、2.3(1.58)）。

e) システムは、まずインストールするソフトウェア パッケージを確認します。現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

yes を入力して、検証に進むことを確認します。

f) インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

FXOS がバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

g) アップグレードプロセスをモニタするには、アップグレード進行のモニタ （197 ページ）を参照してください。

ステップ 3 すべてのコンポーネントが正常にアップグレードされたら、続行する前に、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します（インストールの確認 （198 ページ） を参照してください）。

ステップ 4 シャーシに新しい ASA ソフトウェア イメージをダウンロードします。

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) アプリケーション ソフトウェア モードを開始します。

scope app-software

c) 論理デバイス ソフトウェア イメージをダウンロードします。

download image *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@server/path*
- **scp**://*username@server/path*
- **sftp**://*username@server/path*
- **tftp**://*server:port-num/path*

d) ダウンロード プロセスをモニタする場合：

show download-task

e) ダウンロードしたアプリケーションを表示する場合：

up

show app

ダウンロードしたソフトウェアパッケージの ASA のバージョンをメモします。後の手順でアプリケーションを有効にするために、正確なバージョン文字列を使用する必要があります。

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State

    ---------------------------- ---------- -------------------- --------------- -----

    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1          user
Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

ステップ 5 ASA 論理デバイス イメージのアップグレード：

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) スコープを更新するセキュリティ モジュールに設定します。

scope slot*slot_number*

c) スコープを更新する ASA アプリケーションに設定します。

FXOS 2.3.1 以前： **scope app-instance asa**

FXOS 2.4.1 以降：**scope app-instance asa** *instance_name*

d) スタートアップ バージョンを更新するバージョンに設定します。

set startup-version *version_number*

e) 設定をコミットします。

commit-buffer

トランザクションをシステムの設定にコミットします。アプリケーションイメージが更新され、アプリケーションが再起動します。

ステップ 6 セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認するには、インストールの確認 （198 ページ） を参照してください。

ステップ 7 アップグレードしたユニットをアクティブユニットにして、アップグレード済みのユニットにトラフィックが流れるようにします。

a) スタンバイ ASA 論理デバイスが含まれる Firepower セキュリティ アプライアンスで、コンソール接続または Telnet 接続を使用してモジュール CLI に接続します。

connect module *slot_number* {**console** | **telnet**}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) アプリケーションのコンソールに接続します。

connect asa

例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) この装置をアクティブにします。

failover active

d) 設定を保存します。

write memory

e) ユニットがアクティブであることを確認します。

show failover

ステップ 8 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

Ctrl-a, d と入力します。

ステップ 9 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

ステップ 10 新しいスタンバイ ASA 論理デバイスが含まれている Firepower セキュリティ アプライアンスでは、新しい FXOS プラットフォーム バンドル イメージとをアップロードします：

a) FXOS CLI に接続します。

b) ファームウェア モードを開始します。

scope firmware

c) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

download image *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@server*/*path*/*image_name*
- **scp**://*username@server*/*path*/*image_name*
- **sftp**://*username@server*/*path*/*image_name*
- **tftp**://*server***:***port-num*/*path*/*image_name*

d) ダウンロード プロセスをモニタする場合：

scope download-task *image_name*

show detail

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
```

```
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

ステップ 11 新しいFXOSプラットフォームバンドルのイメージが正常にダウンロードされたら、FXOSバンドルをアップグレードします。

a) 必要に応じて、ファームウェア モードに戻ります。

up

b) インストールする FXOS プラットフォーム バンドルのバージョン番号をメモします。

show package

c) auto-install モードにします。

scope auto-install

d) FXOS プラットフォーム バンドルをインストールします。

install platform platform-vers *version_number*

version_number は、インストールする FXOS プラットフォーム バンドルのバージョン番号です（たとえば、2.3(1.58)）。

e) システムは、まずインストールするソフトウェア パッケージを確認します。現在インストールされているアプリケーションと指定したFXOSプラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

yes を入力して、検証に進むことを確認します。

f) インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

FXOS がバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

g) アップグレードプロセスをモニタするには、アップグレード進行のモニタ （197 ページ）を参照してください。

ステップ 12 すべてのコンポーネントが正常にアップグレードされたら、続行する前に、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します（インストールの確認 （198 ページ） を参照してください）。

ステップ 13 シャーシに新しい ASA ソフトウェア イメージをダウンロードします。

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) アプリケーション ソフトウェア モードを開始します。

scope app-software

c) 論理デバイス ソフトウェア イメージをダウンロードします。

download image *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@server*/*path*
- **scp**://*username@server*/*path*
- **sftp**://*username@server*/*path*
- **tftp**://*server*:*port-num*/*path*

d) ダウンロード プロセスをモニタする場合：

show download-task

e) ダウンロードしたアプリケーションを表示する場合：

up

show app

ダウンロードしたソフトウェアパッケージの ASA のバージョンをメモします。後の手順でアプリケーションを有効にするために、正確なバージョン文字列を使用する必要があります。

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State

    ----------------------------- ---------- -------------------- --------------- -----

    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1          user
Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

ステップ 14 ASA 論理デバイス イメージのアップグレード：

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) スコープを更新するセキュリティ モジュールに設定します。

scope slot*slot_number*

c) スコープを更新する ASA アプリケーションに設定します。

FXOS 2.3.1 以前： **scope app-instance asa**

FXOS 2.4.1 以降：**scope app-instance asa** *instance_name*

d) スタートアップ バージョンを更新するバージョンに設定します。

set startup-version *version_number*

e) 設定をコミットします。

commit-buffer

トランザクションをシステムの設定にコミットします。アプリケーション イメージが更新され、アプリケーションが再起動します。

ステップ 15 セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認するには、インストールの確認 （198 ページ） を参照してください。

ステップ 16 （オプション）アップグレードしたユニットを、アップグレード前のようにアクティブ ユニットにします。

a) スタンバイ ASA 論理デバイスが含まれる Firepower セキュリティ アプライアンスで、コンソール接続または Telnet 接続を使用してモジュール CLI に接続します。

connect module *slot_number* {**console** | **telnet**}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) アプリケーションのコンソールに接続します。

connect asa

例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
```

```
asa>
```

c) この装置をアクティブにします。

failover active

d) 設定を保存します。

write memory

e) ユニットがアクティブであることを確認します。

show failover

FXOS および ASA アクティブ/アクティブ フェールオーバー ペアのアップグレード

FXOS CLI または Firepower Chassis Manager を使用して、FXOS および ASA アクティブ/アクティブ フェールオーバー ペアをアップグレードします。

Firepower Chassis Manager を使用した FXOS および ASA アクティブ/アクティブ フェールオーバー ペアのアップグレード

アップグレード プロセスはシャーシごとに最大 45 分かかることがあります。適切なアップグレード活動の計画を行ってください。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- どのユニットがプライマリ ユニットか特定する必要があります。ASDM に接続し、**[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** の順に選択して、このユニットの優先順位（プライマリまたはセカンダリ）を表示し、接続先のユニットを確認できるようにします。
- アップグレード先の FXOS および ASA ソフトウェア パッケージをダウンロードします（Cisco.com からのソフトウェアのダウンロード （51 ページ）を参照してください）。
- FXOS と ASA の構成をバックアップします。

手順

ステップ 1 プライマリ ユニットの両方のフェールオーバー グループをアクティブにします。

a) フェールオーバー グループ 1 の管理アドレスに接続して、プライマリ ユニット（またはフェールオーバー グループ 1 がアクティブに設定されているユニット）で ASDM を起動します。
b) **[モニタリング（Monitoring）] > [フェールオーバー（Failover）] > [フェールオーバー グループ 2（Failover Group 2）]** の順に選択して、[アクティブにする（Make Active）] をクリックします。
c) 後続の手順のために、このユニットの ASDM に接続したままにします。

ステップ 2 セカンダリ ASA 論理デバイスが含まれている Firepower セキュリティ アプライアンスでは、新しい FXOS プラットフォーム バンドル イメージと ASA ソフトウェア イメージをアップロードします：

（注） FXOS 2.3.1 より前のバージョンにアップグレードする場合、FXOS プラットフォーム バンドル ソフトウェアをアップグレードするまでは、ASA CSP イメージをセキュリティ アプライアンスにアップロードしないでください。

a) セカンダリ ユニットの Firepower Chassis Manager に接続します。
b) **[System] > [Updates]** を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。
c) [Upload Image] をクリックします。
d) [Choose File] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。
e) [Upload] をクリックします。
選択したイメージがシャーシにアップロードされます。

ステップ 3 新しい FXOS プラットフォーム バンドル イメージが正常にアップロードされた後に、セカンダリ ASA 論理デバイスが含まれている Firepower セキュリティ アプライアンスの FXOS バンドルをアップグレードします。

a) アップグレードする FXOS プラットフォーム バンドルの [Upgrade] アイコンをクリックします。

システムは、まずインストールするソフトウェア パッケージを確認します。現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

b) [はい（Yes）] をクリックして、インストールを続行することを確認します。

FXOS がバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 4 Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレードプロセスをモニタできます（アップグレード進行のモニタ （197 ページ） を参照してください）。

ステップ 5 すべてのコンポーネントが正常にアップグレードされたら、続行する前に、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します（インストールの確認 （198 ページ） を参照してください）。

ステップ 6 ASA 論理デバイス イメージのアップグレード：

a) [論理デバイス（Logical Devices）] を選択します。
[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。

b) 更新する論理デバイスの [Set Version] アイコンをクリックして、[Update Image Version] ダイアログボックスを開きます。

c) [New Version] では、更新後のソフトウェア バージョンを選択します。

d) [OK] をクリックします。

ステップ 7 アップグレードプロセスが完了したら、アプリケーションがオンラインであり、正常にアップグレードされたことを確認します。

a) [論理デバイス（Logical Devices）] を選択します。

b) アプリケーションのバージョンと動作ステータスを確認します。

ステップ 8 セカンダリ ユニットの両方のフェールオーバー グループをアクティブにします。

a) フェールオーバー グループ 1 の管理アドレスに接続して、プライマリ ユニット（またはフェールオーバー グループ 1 がアクティブに設定されているユニット）で ASDM を起動します。

b) **[Monitoring]** > **[Failover]** > **[Failover Group 1]** の順に選択して、[Make Standby] をクリックします。

c) **[Monitoring]** > **[Failover]** > **[Failover Group 2]** の順に選択して、[Make Standby] をクリックします。

ASDM は、セカンダリ ユニット上のフェールオーバー グループ 1 の IP アドレスに自動的に再接続されます。

ステップ 9 プライマリ ASA 論理デバイスが含まれている Firepower セキュリティ アプライアンスでは、新しい FXOS プラットフォーム バンドル イメージと ASA ソフトウェア イメージをアップロードします：

（注） FXOS 2.3.1 より前のバージョンにアップグレードする場合、FXOS プラットフォーム バンドル ソフトウェアをアップグレードするまでは、ASA CSP イメージをセキュリティ アプライアンスにアップロードしないでください。

a) プライマリ ユニットの Firepower Chassis Manager に接続します。

b) **[System]** > **[Updates]** を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。

c) [Upload Image] をクリックして、[Upload Image] ダイアログボックスを開きます。

d) [Choose File] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。

e) [Upload] をクリックします。
選択したパッケージがシャーシにアップロードされます。

f) 特定のソフトウェア イメージの場合、イメージのアップロード後にエンドユーザ ライセンス契約書が表示されます。システム プロンプトに従って、エンド ユーザ ライセンス契約書に同意します。

ステップ 10 新しい FXOS プラットフォーム バンドル イメージが正常にアップロードされた後に、プライマリ ASA 論理デバイスが含まれている Firepower セキュリティ アプライアンスの FXOS バンドルをアップグレードします。

a) アップグレードする FXOS プラットフォーム バンドルの [Upgrade] アイコンをクリックします。

システムは、まずインストールするソフトウェア パッケージを確認します。現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

b) [はい（Yes）] をクリックして、インストールを続行することを確認します。

FXOS がバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 11 Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレードプロセスをモニタできます（アップグレード進行のモニタ （197ページ） を参照してください）。

ステップ 12 すべてのコンポーネントが正常にアップグレードされたら、続行する前に、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します（インストールの確認 （198 ページ） を参照してください）。

ステップ 13 ASA 論理デバイス イメージのアップグレード：

a) [論理デバイス（Logical Devices）] を選択します。
[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。

b) 更新する論理デバイスの [Set Version] アイコンをクリックして、[Update Image Version] ダイアログボックスを開きます。

c) [New Version] では、更新後のソフトウェア バージョンを選択します。

d) [OK] をクリックします。

ステップ 14 アップグレードプロセスが完了したら、アプリケーションがオンラインであり、正常にアップグレードされたことを確認します。

a) [論理デバイス（Logical Devices）] を選択します。

b) アプリケーションのバージョンと動作ステータスを確認します。

ステップ 15 フェールオーバー グループは、[Preempt Enabled] を使用して設定されると、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。[Preempt Enabled] でフェールオーバー グループが設定されていない場合は、[Monitoring] > [Failover] > [Failover Group #] ペインを使用して、指定された装置上でアクティブ ステータスに戻すことができます。

FXOS CLI を使用した FXOS および ASA アクティブ/アクティブ フェールオーバー ペアのアップグレード

アップグレード プロセスはシャーシごとに最大 45 分かかることがあります。適切なアップグレード活動の計画を行ってください。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- どのユニットがプライマリかを特定する必要があります。Firepower セキュリティ アプライアンスで ASA コンソールに接続し、**show failover** コマンドを入力してユニットの状態と優先順位（プライマリまたはセカンダリ）を表示します。
- アップグレード先の FXOS および ASA ソフトウェア パッケージをダウンロードします（Cisco.com からのソフトウェアのダウンロード （51 ページ）を参照してください）。
- FXOS と ASA の構成をバックアップします。
- シャーシにソフトウェア イメージをダウンロードするために必要な次の情報を収集します。
  - イメージのコピー元のサーバの IP アドレスおよび認証クレデンシャル。
  - イメージ ファイルの完全修飾名。

手順

ステップ 1 コンソール ポート（推奨）または SSH を使用して、セカンダリ ユニットの FXOS CLI に接続します。

ステップ 2 プライマリ ユニットの両方のフェールオーバー グループをアクティブにします。

a) コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

connect module *slot_number* {**console** | **telnet**}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) アプリケーションのコンソールに接続します。

connect asa

例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) プライマリ ユニットの両方のフェールオーバー グループをアクティブにします。

enable

デフォルトで、イネーブル パスワードは空白です。

no failover active group 1

no failover active group 2

例：

```
asa> enable
Password: <blank>
asa# no failover active group 1
asa# no failover active group 2
```

ステップ 3 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

Ctrl-a, d と入力します。

ステップ 4 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) **~** と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

ステップ 5 セカンダリ ASA 論理デバイスが含まれている Firepower セキュリティ アプライアンスでは、新しいFXOSプラットフォームバンドルイメージとASAソフトウェアイメージをダウンロードします：

a) FXOS CLI に接続します。

b) ファームウェア モードを開始します。

scope firmware

c) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

download image *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@server*/*path*/*image_name*
- **scp**://*username@server*/*path*/*image_name*
- **sftp**://*username@server*/*path*/*image_name*
- **tftp**://*server*:*port-num*/*path*/*image_name*

d) ダウンロード プロセスをモニタする場合：

scope download-task *image_name*

show detail

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

ステップ 6 新しいFXOSプラットフォーム バンドルのイメージが正常にダウンロードされたら、FXOS バンドルをアップグレードします。

a) 必要に応じて、ファームウェア モードに戻ります。

top

scope firmware

b) インストールする FXOS プラットフォーム バンドルのバージョン番号をメモします。

show package

c) auto-install モードにします。

scope auto-install

d) FXOS プラットフォーム バンドルをインストールします。

install platform platform-vers *version_number*

version_number は、インストールする FXOS プラットフォーム バンドルのバージョン番号です（たとえば、2.3(1.58)）。

e) システムは、まずインストールするソフトウェア パッケージを確認します。現在インストールされているアプリケーションと指定したFXOSプラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

yes を入力して、検証に進むことを確認します。

f) インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

FXOS がバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

g) アップグレードプロセスをモニタするには、アップグレード進行のモニタ （197 ページ）を参照してください。

ステップ 7 すべてのコンポーネントが正常にアップグレードされたら、続行する前に、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します（インストールの確認 （198 ページ） を参照してください）。

ステップ 8 シャーシに新しい ASA ソフトウェア イメージをダウンロードします。

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) アプリケーション ソフトウェア モードを開始します。

scope app-software

c) 論理デバイス ソフトウェア イメージをダウンロードします。

download image *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@server/path*
- **scp**://*username@server/path*
- **sftp**://*username@server/path*
- **tftp**://*server:port-num/path*

d) ダウンロード プロセスをモニタする場合：

show download-task

e) ダウンロードしたアプリケーションを表示する場合：

up

show app

ダウンロードしたソフトウェアパッケージの ASA のバージョンをメモします。後の手順でアプリケーションを有効にするために、正確なバージョン文字列を使用する必要があります。

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State

    ----------------------------- ---------- -------------------- --------------- -----

    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1          user
Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

ステップ 9 ASA 論理デバイス イメージのアップグレード：

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) スコープを更新するセキュリティ モジュールに設定します。

scope slot*slot_number*

c) スコープを更新する ASA アプリケーションに設定します。

FXOS 2.3.1 以前： **scope app-instance asa**

FXOS 2.4.1 以降：**scope app-instance asa** *instance_name*

d) スタートアップ バージョンを更新するバージョンに設定します。

set startup-version *version_number*

e) 設定をコミットします。

commit-buffer

トランザクションをシステムの設定にコミットします。アプリケーション イメージが更新され、アプリケーションが再起動します。

ステップ 10 セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認するには、インストールの確認 （198 ページ） を参照してください。

ステップ 11 セカンダリ ユニットの両方のフェールオーバー グループをアクティブにします。

a) コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

connect module *slot_number* {**console** | **telnet**}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) アプリケーションのコンソールに接続します。

connect asa

例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) セカンダリ ユニットの両方のフェールオーバー グループをアクティブにします。

enable

デフォルトで、イネーブル パスワードは空白です。

failover active group 1

failover active group 2

例：

```
asa> enable
Password: <blank>
asa# failover active group 1
asa# failover active group 2
```

ステップ 12 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

Ctrl-a, d と入力します。

ステップ 13 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

ステップ 14 プライマリ ASA 論理デバイスが含まれる Firepower セキュリティ アプライアンスで、新しい FXOS プラットフォーム バンドルのイメージと ASA ソフトウェア イメージをダウンロードします。

a) FXOS CLI に接続します。

b) ファームウェア モードを開始します。

scope firmware

c) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

download image *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@server*/*path*/*image_name*
- **scp**://*username@server*/*path*/*image_name*
- **sftp**://*username@server*/*path*/*image_name*
- **tftp**://*server***:***port-num*/*path*/*image_name*

d) ダウンロード プロセスをモニタする場合：

scope download-task *image_name*

show detail

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
```

```
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

ステップ 15 新しいFXOSプラットフォーム バンドルのイメージが正常にダウンロードされたら、FXOSバンドルをアップグレードします。

a) 必要に応じて、ファームウェア モードに戻ります。

up

b) インストールする FXOS プラットフォーム バンドルのバージョン番号をメモします。

show package

c) auto-install モードにします。

scope auto-install

d) FXOS プラットフォーム バンドルをインストールします。

install platform platform-vers *version_number*

version_number は、インストールする FXOS プラットフォーム バンドルのバージョン番号です（たとえば、2.3(1.58)）。

e) システムは、まずインストールするソフトウェア パッケージを確認します。現在インストールされているアプリケーションと指定したFXOSプラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

yes を入力して、検証に進むことを確認します。

f) インストールの続行を確定するには**yes**を、インストールをキャンセルするには**no**を入力します。

FXOS がバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

g) アップグレードプロセスをモニタするには、アップグレード進行のモニタ （197 ページ）を参照してください。

ステップ 16 すべてのコンポーネントが正常にアップグレードされたら、続行する前に、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します（インストールの確認 （198 ページ） を参照してください）。

ステップ 17 シャーシに新しい ASA ソフトウェア イメージをダウンロードします。

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) アプリケーション ソフトウェア モードを開始します。

scope app-software

c) 論理デバイス ソフトウェア イメージをダウンロードします。

download image *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@server*/*path*
- **scp**://*username@server*/*path*
- **sftp**://*username@server*/*path*
- **tftp**://*server*:*port-num*/*path*

d) ダウンロード プロセスをモニタする場合：

show download-task

e) ダウンロードしたアプリケーションを表示する場合：

up

show app

ダウンロードしたソフトウェアパッケージの ASA のバージョンをメモします。後の手順でアプリケーションを有効にするために、正確なバージョン文字列を使用する必要があります。

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State

    ----------------------------- ---------- -------------------- --------------- -----

    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1          user
Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

ステップ 18 ASA 論理デバイス イメージのアップグレード：

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) スコープを更新するセキュリティ モジュールに設定します。

scope slot*slot_number*

c) スコープを更新する ASA アプリケーションに設定します。

FXOS 2.3.1 以前： **scope app-instance asa**

FXOS 2.4.1 以降：**scope app-instance asa** *instance_name*

d) スタートアップ バージョンを更新するバージョンに設定します。

set startup-version *version_number*

e) 設定をコミットします。

commit-buffer

トランザクションをシステムの設定にコミットします。アプリケーション イメージが更新され、アプリケーションが再起動します。

ステップ 19 セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認するには、インストールの確認 （198 ページ） を参照してください。

ステップ 20 フェールオーバー グループは、[Preempt Enabled] を使用して設定されると、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。[Preempt Enabled] でフェールオーバー グループが設定されていない場合は、[Monitoring] > [Failover] > [Failover Group #] ペインを使用して、指定された装置上でアクティブ ステータスに戻すことができます。

FXOS および ASA シャーシ間クラスタのアップグレード

FXOS CLI または Firepower Chassis Manager を使用して、シャーシ間クラスタ内のすべてのシャーシの FXOS と ASA をアップグレードします。

Firepower Chassis Manager を使用した FXOS および ASA シャーシ間クラスタのアップグレード

アップグレード プロセスはシャーシごとに最大 45 分かかることがあります。適切なアップグレード活動の計画を行ってください。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS および ASA ソフトウェア パッケージをダウンロードします（Cisco.com からのソフトウェアのダウンロード （51 ページ）を参照してください）。
- FXOS と ASA の構成をバックアップします。

手順

ステップ 1 どのシャーシが制御ユニットかを決定します。このシャーシは最終にアップグレードします。

a) Firepower Chassis Manager に接続します。
b) [論理デバイス（Logical Devices）] を選択します。
c) クラスタに含まれるセキュリティ モジュールの属性を表示するには、プラス記号（+）をクリックします。
d) 制御ユニットがこのシャーシ上にあることを確認します。**CLUSTER-ROLE** が「Master」に設定されている ASA インスタンスがあるはずです。

ステップ 2 制御ユニットがないクラスタ内のシャーシの Firepower Chassis Manager に接続します。

ステップ 3 新しい FXOS プラットフォーム バンドルのイメージと ASA ソフトウェア イメージのアップロード：

（注） FXOS 2.3.1 より前のバージョンにアップグレードする場合、FXOS プラットフォーム バンドル ソフトウェアをアップグレードするまでは、ASA CSP イメージをセキュリティ アプライアンスにアップロードしないでください。

a) Firepower Chassis Manager で、**[システム（System）] > [更新（Updates）]** を選択します。[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。
b) [Upload Image] をクリックします。
c) [Choose File] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。
d) [Upload] をクリックします。
選択したイメージがシャーシにアップロードされます。
e) 続行する前に、イメージが正常にアップロードされるまで待ちます。

ステップ 4 （FXOS 2.4.1 以前）シャーシのすべてのセキュリティモジュールでクラスタリングを無効にします。

注：FXOS バージョン 2.6.1 以降からアップグレードする場合は、この手順をスキップできます。

a) [論理デバイス（Logical Devices）] を選択します。
b) 各アプリケーションの [Disable] スライダをクリックして、クラスタ内に含まれている各アプリケーション インスタンスを無効にします。
[Cluster Operational Status] が not-in-cluster に変化します。

ステップ 5 FXOS バンドルのアップグレード：

a) [System] > [Updates] を選択します。
b) アップグレードする FXOS プラットフォーム バンドルの [Upgrade] アイコンをクリックします。

システムは、まずインストールするソフトウェア パッケージを確認します。現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。ASA バー

ジョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

c) [はい（Yes）] をクリックして、インストールを続行することを確認します。

FXOS がバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 6 Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレードプロセスをモニタできます（アップグレード進行のモニタ （197ページ） を参照してください）。

ステップ 7 すべてのコンポーネントが正常にアップグレードされたら、続行する前に、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します（インストールの確認 （198 ページ） を参照してください）。

ステップ 8 各セキュリティモジュールでの ASA 論理デバイス イメージのアップグレード：

a) [論理デバイス（Logical Devices）] を選択します。
[Logical Devices]ページに、シャーシに設定された論理デバイスのリストが表示されます。

b) 更新する論理デバイスの [Set Version] アイコンをクリックして、[Update Image Version] ダイアログボックスを開きます。

c) [New Version] では、更新後のソフトウェア バージョンを選択します。

d) [OK] をクリックします。

ステップ 9 アップグレードプロセスが完了したら、アプリケーションがオンラインであり、正常にアップグレードされたことを確認します。

a) [論理デバイス（Logical Devices）] を選択します。

b) アプリケーションのバージョンと動作ステータスを確認します。

ステップ 10 （FXOS 2.4.1 以前）シャーシのすべてのセキュリティモジュールでクラスタリングを再度有効にします。

注：FXOS バージョン 2.6.1 以降からアップグレードする場合は、この手順をスキップできます。

a) [論理デバイス（Logical Devices）] を選択します。

b) クラスタに含まれる各セキュリティモジュールの [Enable] スイッチをクリックします。
[Cluster Operational Status] が in-cluster に変化します。

ステップ 11 制御ユニットがないクラスタ内の残りのすべてのシャーシで、手順 2 ～ 10 を繰り返します。

ステップ 12 制御ユニットを持たないクラスタ内のすべてのシャーシがアップグレードされたら、最初にデータユニットでクラスタリングを無効にしてから、最後に制御ユニットを無効にしたことを確認し、シャーシ上で制御ユニットを使用して手順 2 ー 10 を繰り返します。
新しい制御ユニットが、以前にアップグレードされたシャーシのいずれかから選択されます。

ステップ 13 クラスタが安定したら、制御ユニットで ASA コンソールを使用して、クラスタ内のすべてのモジュール間でアクティブ セッションを再配布します。

cluster redistribute vpn-sessiondb

次のタスク

シャーシのサイト ID を設定します。シャーシのサイト ID を設定する方法の詳細については、Cisco.com で『Deploying a Cluster for ASA for the Firepower 4100/9300 for Scalability and High Availability』の「Inter-Site Clustering」トピックを参照してください。

FXOS CLI を使用した FXOS および ASA シャーシ間クラスタの FXOS のアップグレード

アップグレード プロセスはシャーシごとに最大 45 分かかることがあります。適切なアップグレード活動の計画を行ってください。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS および ASA ソフトウェア パッケージをダウンロードします（Cisco.com からのソフトウェアのダウンロード （51 ページ）を参照してください）。
- FXOS と ASA の構成をバックアップします。
- シャーシにソフトウェア イメージをダウンロードするために必要な次の情報を収集します。
  - イメージのコピー元のサーバの IP アドレスおよび認証クレデンシャル。
  - イメージ ファイルの完全修飾名。

手順

ステップ 1 どのシャーシが制御ユニットかを決定します。このシャーシは最終にアップグレードします。

a) FXOS CLI に接続します。

b) 制御ユニットがこのシャーシ上にあることを確認します。Cluster Role が「Master」に設定されている ASA インスタンスがあるはずです。

scope ssa

show app-instance

ステップ 2 制御ユニットがないクラスタ内のシャーシの FXOS CLI に接続します。

ステップ 3 新しいプラットフォーム バンドル イメージをシャーシにダウンロードします。

a) ファームウェア モードを開始します。

scope firmware

b) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

download image *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@server*/*path*/*image_name*
- **scp**://*username@server*/*path*/*image_name*
- **sftp**://*username@server*/*path*/*image_name*
- **tftp**://*server*:*port-num*/*path*/*image_name*

c) ダウンロード プロセスをモニタする場合：

scope download-task *image_name*

show detail

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

ステップ 4 新しい FXOS プラットフォーム バンドル イメージが正常にダウンロードされた後、シャーシのすべてのセキュリティ モジュールでクラスタリングを無効にします。

a) コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

connect module *slot_number* {**console** | **telnet**}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) アプリケーションのコンソールに接続します。

connect asa

例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) いずれかのすべてのセキュリティ モジュールでクラスタリングを無効にします。

cluster group *name*

no enable

このシャーシ上の FXOS と ASA をアップグレードする場合は、シャーシの再起動後にクラスタリングが無効になるように設定を保存します。

write memory

d) クラスタが安定するのを待ちます。すべてのバックアップセッションが作成されたことを確認してください。

show cluster vpn-sessiondb summary

e) このシャーシ上のセキュリティ モジュールごとに、手順 4 を繰り返します。

ステップ 5 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

Ctrl-a, d と入力します。

ステップ 6 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) **~** と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

ステップ 7 FXOS バンドルをアップグレードします。

a) 必要に応じて、ファームウェア モードに戻ります。

top

scope firmware

b) インストールする FXOS プラットフォーム バンドルのバージョン番号をメモします。

show package

c) auto-install モードにします。

scope auto-install

d) FXOS プラットフォーム バンドルをインストールします。

install platform platform-vers *version_number*

version_number は、インストールする FXOS プラットフォーム バンドルのバージョン番号です（たとえば、2.3(1.58)）。

e) システムは、まずインストールするソフトウェア パッケージを確認します。現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

yes を入力して、検証に進むことを確認します。

f) インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

FXOS がバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

g) アップグレードプロセスをモニタするには、アップグレード進行のモニタ （197 ページ）を参照してください。

ステップ 8 すべてのコンポーネントが正常にアップグレードされたら、続行する前に、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します（インストールの確認 （198 ページ） を参照してください）。

ステップ 9 シャーシに新しい ASA ソフトウェア イメージをダウンロードします。

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) アプリケーション ソフトウェア モードを開始します。

scope app-software

c) 論理デバイス ソフトウェア イメージをダウンロードします。

download image *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@server/path*
- **scp**://*username@server/path*
- **sftp**://*username@server/path*
- **tftp**://*server:port-num/path*

d) ダウンロード プロセスをモニタする場合：

show download-task

e) ダウンロードしたアプリケーションを表示する場合：

up

show app

ダウンロードしたソフトウェアパッケージの ASA のバージョンをメモします。後の手順でアプリケーションを有効にするために、正確なバージョン文字列を使用する必要があります。

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State

    ----------------------------- ---------- -------------------- --------------- -----

    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1          user
Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

ステップ 10 ASA 論理デバイス イメージのアップグレード：

a) セキュリティ サービス モードを開始します。

top

scope ssa

b) スコープを更新するセキュリティ モジュールに設定します。

scope slot*slot_number*

c) スコープを更新する ASA アプリケーションに設定します。

FXOS 2.3.1 以前： **scope app-instance asa**

FXOS 2.4.1 以降：**scope app-instance asa** *instance_name*

d) スタートアップ バージョンを更新するバージョンに設定します。

set startup-version *version_number*

e) 設定をコミットします。

commit-buffer

トランザクションをシステムの設定にコミットします。アプリケーションイメージが更新され、アプリケーションが再起動します。

ステップ 11 セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認するには、インストールの確認 （198 ページ） を参照してください。

ステップ 12 アップグレードされたセキュリティモジュールがオンラインになった後、シャーシのすべてのセキュリティ モジュールでクラスタリング再度有効にします。

a) コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

connect module *slot_number* {**console** | **telnet**}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) アプリケーションのコンソールに接続します。

connect asa

例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) いずれかのすべてのセキュリティ モジュールでクラスタリングを無効にします。

cluster group *name*

enable

write memory

d) このシャーシ上のセキュリティ モジュールごとに、手順 12 を繰り返します。

ステップ 13 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

Ctrl-a, d と入力します。

ステップ 14 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

ステップ 15 制御ユニットがないクラスタ内の残りのすべてのシャーシで、手順 2 ～ 14 を繰り返します。

ステップ 16 制御ユニットを持たないクラスタ内のすべてのシャーシがアップグレードされたら、最初にデータユニットでクラスタリングを無効にしてから、最後に制御ユニットを無効にしたことを確認し、シャーシ上で制御ユニットを使用して手順 2 ー 14 を繰り返します。
新しい制御ユニットが、以前にアップグレードされたシャーシのいずれかから選択されます。

ステップ 17 クラスタが安定したら、制御ユニットで ASA コンソールを使用して、クラスタ内のすべてのモジュール間でアクティブ セッションを再配布します。

cluster redistribute vpn-sessiondb

次のタスク

シャーシのサイト ID を設定します。シャーシのサイト ID を設定する方法の詳細については、Cisco.com で『Deploying a Cluster for ASA for the Firepower 4100/9300 for Scalability and High Availability』の「Inter-Site Clustering」トピックを参照してください。

アップグレード進行のモニタ

FXOS CLI を使用してアップグレード プロセスをモニタできます。

手順

ステップ 1 FXOS CLI に接続します。

ステップ 2 **scope system** を入力します。

ステップ 3 **show firmware monitor** を入力します。

ステップ 4 すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「`Upgrade-Status: Ready`」と表示されるのを待ちます。

（注） FPRMコンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例

```
Firepower-chassis# scope system
Firepower-chassis /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

インストールの確認

次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

手順

ステップ 1 FXOS CLI に接続します。

ステップ 2 **top** を入力します。

ステップ 3 **scope ssa** を入力します。

ステップ 4 **show slot** を入力します。

ステップ 5 Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。

例：

ステップ 6 **show app-instance** を入力します。

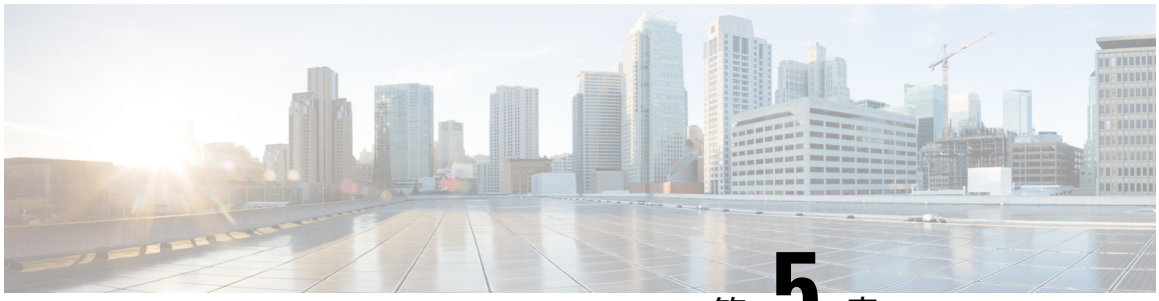
ステップ 7 シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であり、正しいバージョンがリストされていることを確認します。

このシャーシがクラスタの一部である場合、シャーシにインストールされているすべてのセキュリティモジュールで、クラスタ動作状態が「In-Cluster」であることを確認します。また、制御ユニットがアップグレードするシャーシ上にないことを確認します。Cluster Role が「Master」に設定されているインスタンスがあってはいけません。

例

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
Firepower-chassis /ssa #
Firepower-chassis /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup
Version Cluster State   Cluster Role
---------- ---------- ---------- ----------- ----------------- ---------------
--------------- --------------- ------------
asa        asa1       1          Enabled     Online           9.10.0.85       9.10.0.85
       Not Applicable  None
asa        asa2       2          Enabled     Online           9.10.0.85       9.10.0.85
       Not Applicable  None
Firepower-chassis /ssa #
```



第 5 章

ASA のダウングレード

多くの場合、ASA ソフトウェアをダウングレードし、以前のソフトウェアバージョンからバックアップ設定を復元することができます。ダウングレードの方法は、ASA プラットフォームによって異なります。

ダウングレードに関するガイドラインおよび制限事項

ダウングレードする前に、次のガイドラインを参照してください。

- クラスタリング用の公式のゼロ ダウンタイム ダウングレードのサポートはありません。ただし場合によっては、ゼロ ダウンタイム ダウングレードが機能します。ダウングレードに関する次の既知の問題を参照してください。この他の問題が原因でクラスタ ユニットのリロードが必要になることもあり、その場合はダウンタイムが発生します。
  - クラスタリングを含む 9.9(1) より前のリリースへのダウングレード：9.9(1) 以降では、バックアップの配布が改善されています。クラスタに 3 つ以上のユニットがある場合は、次の手順を実行する必要があります。
    1. クラスタからすべてのセカンダリ ユニットを削除します（クラスタはプライマリ ユニットのみで構成されます）。
    2. 1 つのセカンダリ ユニットをダウングレードし、クラスタに再参加させます。
    3. プライマリ ユニットでクラスタリングを無効にします。そのユニットをダウングレードし、クラスタに再参加させます。
    4. 残りのセカンダリ ユニットをダウングレードし、それらを一度に 1 つずつクラスタに再参加させます。

- クラスタ サイトの冗長性を有効にする場合は、9.9(1) より前のリリースにダウングレードします。ダウングレードする場合（または 9.9(1) より前のユニットをクラスタに追加する場合）は、サイトの冗長性を無効にする必要があります。そうしないと、古いバージョンを実行しているユニットにダミーの転送フローなどの副作用が発生します。
- クラスタリングおよび暗号マップを使用する場合に 9.8(1) からダウングレードする：暗号マップが設定されている場合に 9.8 (1) からダウングレードすると、ゼロ ダウンタイム ダウングレードはサポートされません。ダウングレード前に暗号マップ設定をクリアし、ダウングレード後に設定をもう一度適用する必要があります。
- クラスタリング ユニットのヘルスチェックを 0.3 ～ 0.7 秒に設定した状態で 9.8(1) からダウングレードする：（**health-check holdtime** で）ホールド時間を 0.3 ～ 0.7 秒に設定した後で ASA ソフトウェアをダウングレードすると、新しい設定はサポートされないため、設定値はデフォルトの 3 秒に戻ります。
- クラスタリング（CSCuv82933）を使用している場合に 9.5(2) 以降から 9.5(1) 以前にダウングレードする：9.5(2) からダウングレードする場合、ゼロ ダウンタイム ダウングレードはサポートされません。ユニットがオンラインに戻ったときに新しいクラスタが形成されるように、すべてのユニットをほぼ同時にリロードする必要があります。ユニットが順番にリロードされるのを待つと、クラスタを形成できなくなります。
- クラスタリングを使用する場合に 9.2(1) 以降から 9.1 以前にダウングレードする：ゼロ ダウンタイム ダウングレードはサポートされません。

- プラットフォームモードでの 9.13/9.14 から 9.12 以前への Firepower 2100 のダウングレードの問題：プラットフォームモードに変換した 9.13 または 9.14 を新規インストールした Firepower 2100 の場合：9.12 以前にダウングレードすると、FXOS で新しいインターフェイスの設定や、既存のインターフェイスの編集ができなくなります（9.12 以前ではプラットフォームモードのみがサポートされていたことに注意してください）。バージョンを 9.13 以降に戻すか、または FXOS の erase configuration コマンドを使用して設定をクリアする必要があります。この問題は、元々以前のリリースから 9.13 または 9.14 にアップグレードした場合は発生しません。新しいデバイスや再イメージ化されたデバイスなど、新規インストールのみが影響を受けます。（CSCvr19755）
- スマート ライセンスの 9.10(1) からのダウングレード：スマート エージェントの変更により、ダウングレードする場合、デバイスを Cisco Smart Software Manager に再登録する必要があります。新しいスマート エージェントは暗号化されたファイルを使用するので、古いスマート エージェントが必要とする暗号化されていないファイルを使用するために再登録する必要があります。
- PBKDF2（パスワード ベースのキー派生関数 2）ハッシュをパスワードで使用する場合に 9.5 以前のバージョンにダウングレードする：9.6 より前のバージョンは PBKDF2 ハッシュをサポートしていません。9.6(1) では、32 文字より長い **enable** パスワードおよび **username** パスワードで PBKDF2 ハッシュを使用します。9.7(1) では、すべての新しいパスワードは、長さに関わらず PBKDF2 ハッシュを使用します（既存のパスワードは引き続き MD5 ハッシュを使用します）。ダウングレードすると、**enable** パスワードがデフォルト（空

白）に戻ります。ユーザ名は正しく解析されず、**username** コマンドが削除されます。ローカル ユーザをもう一度作成する必要があります。

- ASAv 用のバージョン 9.5(2.200) からのダウングレード：ASAv はライセンス登録状態を保持しません。**license smart register idtoken id_token force** コマンドで再登録する必要があります（ASDM の場合、[Configuration] > [Device Management] > [Licensing] > [Smart Licensing] ページで [Force registration] オプションを使用）。Smart Software Manager から ID トークンを取得します。
- 元のトンネルがネゴシエートした暗号スイートをサポートしないソフトウェアバージョンをスタンバイ装置が実行している場合でも、VPN トンネルがスタンバイ装置に複製されます。このシナリオは、ダウングレード時に発生します。その場合、VPN 接続を切断して再接続してください。

ダウングレード後に削除される互換性のない設定

以前のバージョンにダウングレードすると、それ以降のバージョンで導入されたコマンドは設定から削除されます。ダウングレードする前に、ターゲットバージョンに対して設定を自動的にチェックする方法はありません。新しいコマンドが ASA の新しい機能にいつ追加されたかをリリースごとに表示できます。

show startup-config errors コマンドを使用してダウングレードした後、拒否されたコマンドを表示できます。ラボデバイスでダウングレードを実行できる場合は、実稼働デバイスでダウングレードを実行する前にこのコマンドを使用して効果を事前に確認できます。

場合によっては、ASA はアップグレード時にコマンドを新しいフォームに自動的に移行するため、バージョンによっては新しいコマンドを手動で設定しなかった場合でも、設定の移行によってダウングレードが影響を受けることがあります。ダウングレード時に使用できる古い設定のバックアップを保持することを推奨します。8.3 へのアップグレード時には、バックアップが自動的に作成されます（<old_version>_startup_cfg.sav）。他の移行ではバックアップが作成されません。ダウングレードに影響する可能性がある自動コマンド移行の詳細については、バージョン固有のガイドラインおよび移行 （65 ページ）を参照してください。

ダウングレードに関するガイドラインおよび制限事項（201 ページ）の既知のダウングレードの問題も参照してください。

たとえば、バージョン9.8(2) を実行している ASA には、次のコマンドが含まれています。

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz privilege 15
snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted
auth md5 12:ab:34 priv aes 128 12:ab:34
```

9.0(4) にダウングレードすると、起動時に次のエラーが表示されます。

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0

                                       ^
ERROR: % Invalid input detected at '^' marker.
```

```
username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz pbkdf2 privilege 15
                                                                ^
ERROR: % Invalid input detected at '^' marker.

snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted
auth md5 12:ab:34 priv aes 128 12:ab:34
                                      ^
ERROR: % Invalid input detected at '^' marker.
```

この例では、**access-list extended** コマンドでの **sctp** のサポートがバージョン 9.5(2) で、**username** コマンドでの **pbkdf2** のサポートがバージョン 9.6(1) で、**snmp-server user** コマンドでの **engineID** のサポートがバージョン9.5(3) で追加されました。

アプライアンスモードでのFirepower1000またはFirepower 2100 のダウングレード

ASA のバージョンを古いバージョンに設定し、バックアップ設定をスタートアップ コンフィギュレーションに復元してからリロードすることによって、ASA ソフトウェアのバージョンをダウングレードすることができます。

始める前に

この手順ではアップグレードする前に ASA のバックアップ設定を行う必要があるため、古い設定を復元することができます。古い設定を復元しない場合は、新規または変更された機能を表す互換性のないコマンドが存在する可能性があります。新しいコマンドは、ソフトウェアの古いバージョンをロードすると拒否されます。

手順

ステップ 1 スタンドアロン、フェールオーバー、またはクラスタリング展開のために、アプライアンスモードでの Firepower 1000 および Firepower 2100 のアップグレード （85 ページ）のアップグレード手順を使用して、ASA ソフトウェアの古いバージョンをロードします。この場合は、ASA の新しいバージョンではなく、古いバージョンを指定します。**重要**：まだ ASAをリロードしないでください。

ステップ 2 ASA CLI で、バックアップの ASA 設定をスタートアップ コンフィギュレーションにコピーします。フェールオーバーの場合は、アクティブユニットでこの手順を実行します。この手順では、コマンドをスタンバイ装置に複製します。

copy *old_config_url* **startup-config**

write memory を使用して実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存しないことが重要です。このコマンドは、バックアップ設定を上書きします。

例：

```
ciscoasa# copy disk0:/9.13.1_cfg.sav startup-config
```

ステップ 3 ASA をリロードします。

ASA CLI

reload

ASDM

[Tools] > **[System Reload]** を選択します。

プラットフォームモードでの Firepower 2100 のダウングレード

バックアップ設定をスタートアップ コンフィギュレーションに復元し、ASA のバージョンを古いバージョンに設定してからリロードすることによって、ASA ソフトウェアのバージョンをダウングレードすることができます。

始める前に

この手順ではアップグレードする前に ASA のバックアップ設定を行う必要があるため、古い設定を復元することができます。古い設定を復元しない場合は、新規または変更された機能を表す互換性のないコマンドが存在する可能性があります。新しいコマンドは、ソフトウェアの古いバージョンをロードすると拒否されます。

手順

ステップ 1 ASA CLI で、バックアップの ASA 設定をスタートアップ コンフィギュレーションにコピーします。フェールオーバーの場合は、アクティブユニットでこの手順を実行します。この手順では、コマンドをスタンバイ装置に複製します。

copy *old_config_url* **startup-config**

write memory を使用して実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存しないことが重要です。このコマンドは、バックアップ設定を上書きします。

例：

```
ciscoasa# copy disk0:/9.12.4_cfg.sav startup-config
```

ステップ 2 FXOS では、スタンドアロン、フェールオーバー、またはクラスタリング展開のために、Firepower Chassis Manage または FXOS CLI を使用して、プラットフォームモードでの Firepower 2100 のアップグレード（100 ページ）のアップグレード手順に従い、ASA ソフトウェアの古いバージョンを使います。この場合は、ASA の新しいバージョンではなく、古いバージョンを指定します。

Firepower 4100/9300 のダウングレード

バックアップ設定をスタートアップ コンフィギュレーションに復元し、ASA のバージョンを古いバージョンに設定してからリロードすることによって、ASA ソフトウェアのバージョンをダウングレードすることができます。

始める前に

- この手順ではアップグレードする前に ASA のバックアップ設定を行う必要があるため、古い設定を復元することができます。古い設定を復元しない場合は、新規または変更された機能を表す互換性のないコマンドが存在する可能性があります。新しいコマンドは、ソフトウェアの古いバージョンをロードすると拒否されます。
- ASA の古いバージョンが、FXOS の現在のバージョンと互換性があることを確認します。互換性がない場合は、古い ASA 設定を復元する前に最初の手順として FXOS をダウングレードします。ダウングレードされた FXOS も、（ダウングレードする前に）ASA の現在のバージョンと互換性があることを確認してください。互換性を実現できない場合は、ダウングレードを実行しないことをお勧めします。

手順

ステップ 1 ASA CLI で、バックアップの ASA 設定をスタートアップ コンフィギュレーションにコピーします。フェールオーバーまたはクラスタリングの場合は、アクティブ/制御ユニットでこの手順を実行します。この手順では、コマンドをスタンバイ/データユニットに複製します。

copy *old_config_url* **startup-config**

write memory を使用して実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存しないことが重要です。このコマンドは、バックアップ設定を上書きします。

例：

```
ciscoasa# copy disk0:/9.8.4_cfg.sav startup-config
```

ステップ 2 FXOS では、スタンドアロン、フェールオーバー、またはクラスタリング展開のために、Firepower Chassis Manage または FXOS CLI を使用して、FirePOWER 4100/9300 の ASA をアップグレード（157 ページ）のアップグレード手順に従い、ASA ソフトウェアの古いバージョンを使います。この場合は、ASA の新しいバージョンではなく、古いバージョンを指定します。

ステップ 3 また、FXOS をダウングレードする場合は、スタンドアロン、フェールオーバー、またはクラスタリング展開のために、Firepower Chassis Manager または FXOS CLI を使用して、FirePOWER 4100/9300 の ASA をアップグレード（157 ページ）のアップグレード手順に従い、ASA ソフトウェアの古いバージョンを使います。

ASA 5500-X または ISA 3000 のダウングレード

ダウングレードでは、ASA 5500-X および ISA 3000 モデルで以下の機能を完了するためのショートカットが存在します。

- ブート イメージ コンフィギュレーションのクリア（**clear configure boot**）。
- 古いイメージへのブート イメージの設定（**boot system**）。
- （オプション）新たなアクティベーション キーの入力（**activation-key**）。
- 実行コンフィギュレーションのスタートアップへの保存（**write memory**）。これにより、BOOT 環境変数を古いイメージに設定します。このため、リロードすると古いイメージがロードされます。
- 古いコンフィギュレーションのバックアップをスタートアップ コンフィギュレーションにコピーします（**copy** *old_config_ur* **startup-config**）。
- リロード（**reload**）。

始める前に

- この手順ではアップグレードする前に ASA のバックアップ設定を行う必要があるため、古い設定を復元することができます。
- ASA FirePOWER モジュールのバージョンがインストールされている場合は、ASA の古いバージョンと互換性があることを確認します。FirePOWER モジュールを以前のメジャーバージョンにダウングレードすることはできません。

手順

ステップ 1 **ASA CLI**：ASA 5500-X モデルのみ：ソフトウェアをダウングレードし、古いコンフィギュレーションを復元します。

downgrade [**/noconfirm**] *old_image_url old_config_url* [**activation-key** *old_key*]

例：

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

/noconfirm オプションを指定すると、プロンプトが表示されずにダウングレードされます。*image_url* は、disk0、disk1、tftp、ftp、または smb 上の古いイメージへのパスです。*old_config_url* は、保存された移行前の設定へのパスです。8.3 よりも前のアクティベーション キーに戻る必要がある場合は、そのアクティベーション キーを入力できます。

ステップ 2 **ASDM**：**[Tools]** > **[Downgrade Software]** を選択します。

[Downgrade Software] ダイアログボックスが表示されます。

ステップ 3 ASA イメージの場合、[Select Image File] をクリックします。

[Browse File Locations] ダイアログボックスが表示されます。

ステップ 4 次のいずれかのオプション ボタンをクリックします。

- [Remote Server]：ドロップダウン リストで [ftp]、[smb]、[http] のいずれかを選択し、以前のイメージ ファイルのパスを入力します。
- [Flash File System]：[Browse Flash] をクリックして、ローカル フラッシュ ファイル システムにある以前のイメージ ファイルを選択します。

ステップ 5 [Configuration] で [Browse Flash] をクリックし、移行前の設定ファイルを選択します。

ステップ 6 （任意） バージョン 8.3 よりも前のアクティベーション キーに戻す場合は、[Activation Key] フィールドで以前のアクティベーション キーを入力します。

ステップ 7 [Downgrade] をクリックします。